

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1353814-0

Total Deleted Page(s) = 4
Page 9 ~ Referral/Consult;
Page 10 ~ Referral/Consult;
Page 26 ~ Referral/Consult;
Page 27 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

~~SECRET//NOFORN~~



b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Collected Item Log

Event Title: (U) ~~(S)~~ Midyear Exam

Date: 10/09/2015

Approved By: [Redacted]

b3
b6
b7C
b7E

Drafted By: [Redacted]

Case ID #: [Redacted] (U) ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

~~Reason: 1.4 (b)
Derived From: FBI
NSISC-20090615
Declassify On: 20251231~~

Full Investigation Initiated: 07/10/2015

Collected From: (U) ~~(S)~~ [Redacted]
1100 NY Avenue NW Suite 300
Washington, District Of Columbia 20005

b6
b7C

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Details: No Details Provided

Item Type	Description
1B Digital	(U) (S) Server 882 Dattobackup.com barcode C8470FC11M70024, Pin [Redacted] Collected On: 10/06/2015 Seizing Individual: [Redacted] Collected By: [Redacted] Location Area: NA Specific Location: NA Device Type: Computer Number of Devices Collected: 1

b6
b7C
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U)
Title: ~~(S)~~ Midyear Exam
Re: [Redacted] 10/09/2015

b3
b7E

◆◆

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Collected Item Log

Event Title: (U) ~~(S)~~ MidYear Exam

Date: 10/09/2015

Approved By: [Redacted]

Drafted By: [Redacted]

Case ID #: [Redacted] (U) ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3
b6
b7C
b7E

~~Reason: 1.4(b)
Derived From: FBI
NSISC-20090615
Declassify On: 20251231~~

Full Investigation Initiated: 07/10/2015

Collected From: (U) ~~(S)~~ Katherine Turner
Williams & Connolly LLP
725 12th Street NW
Washington, District Of Columbia

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Details: No Details Provided

Item Type	Description
1B Digital	(U) (S) 1 USB Drive, 128 GB, Black in Color, S/N [Redacted] Collected On: 10/08/2015 Seizing Individual: [Redacted] Collected By: [Redacted] Location Area: Collected via Consent from Equinix Specific Location: 275 Hartz Way, Secaucus, NJ Device Type: USB Micro Storage Device (thumb drive) Number of Devices Collected: 1

b6
b7C
b7E

~~SECRET//NOFORN~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-8645

~~SECRET//NOFORN~~Title: ~~(S)~~ MidYear Exam

Re: [REDACTED] 10/09/2015

b3
b7E

1B Digital (U) ~~(S)~~ 1 Cisco NAS, Model NSS324, S/N QNP14150082, MAC Address [REDACTED]
Collected On: 10/08/2015
Seizing Individual: [REDACTED]
Collected By: [REDACTED]
Location Area: Collected via Consent from Equinix
Specific Location: 275 Hartz Way, Secaucus, NJ
Device Type: Hard Drive
Serial Number: QNP14150082
Number of Devices Collected: 1

b6
b7C
b7E

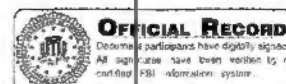
1B Digital (U) ~~(S)~~ 1 Dell PowerEdge R260 Server, Service Tag GXJWFX1, Service Code [REDACTED] Mfg Date [REDACTED]
Collected On: 10/08/2015
Seizing Individual: [REDACTED]
Collected By: [REDACTED]
Location Area: Collected via Consent from Equinix
Specific Location: 275 Hartz Way, Secaucus, NJ
Device Type: Hard Drive
Number of Devices Collected: 1

b6
b7C
b7E

◆◆

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Collected Item Log

Event Title: ~~(S)~~ Midyear Exam

Date: 10/19/2015

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

~~(U)~~ ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3
b6
b7C
b7E

~~Reason: 1.4(b)
Derived From: FBI
NSISC-20090615
Declassify On: 20251231~~

Full Investigation Initiated: 07/10/2015

Collected From: ~~(S)~~ Partner Katherine M. Turner
Williams and Connolly, LLP

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Details: No Details Provided

Item Type	Description
1B Digital	(U) (S) Black Berry 8310, IMEI 359158027424467 Collected On: 10/16/2015 Seizing Individual: [REDACTED] Collected By: [REDACTED] Location Area: NA Specific Location: NA Device Type: Cell Phone Number of Devices Collected: 1

b6
b7C

~~SECRET//NOFORN~~

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

HRC-8647

~~SECRET//NOFORN~~

(U) Title: ~~(S)~~ Midyear Exam

Re: [REDACTED] 10/19/2015

b3
b7E

1B Digital

(U) ~~(S)~~ Black Berry 8700G, IMEI 3576460005545990
 Collected On: 10/16/2015
 Seizing Individual: [REDACTED]
 Collected By: [REDACTED]
 Location Area: NA
 Specific Location: NA
 Device Type: Cell Phone
 Number of Devices Collected: 1

b6
b7C

1B Digital

(U) ~~(S)~~ 32 GB Apple iPad, S/N [REDACTED]
 Collected On: 10/16/2015
 Seizing Individual: [REDACTED]
 Collected By: [REDACTED]
 Location Area: NA
 Specific Location: NA
 Device Type: Cell Phone
 Number of Devices Collected: 1

b6
b7C
b7E

◆◆

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



b3
b7E

FEDERAL BUREAU OF INVESTIGATION
Electronic Communication

Title: (U//~~FOUO~~) Chain of Custody for 1B3

Date: 11/23/2015

From: WASHINGTON FIELD

WF-CI13

Contact: [Redacted]

Approved By: SSA [Redacted]

Drafted By: [Redacted]

Case ID #: [Redacted]

(U) ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) Document the status of the chain of custody for 1B3.

~~Reason: 1.4(b)
Derived From: FBI
NSISC-20090615
Declassify On: 20401231~~

Full Investigation Initiated: 07/10/2015

Reference: [Redacted] Serial 56

Details:

(U//~~FOUO~~) As documented in the referenced serial, on August 12, 2015 the FBI obtained a Dell Poweredge 2900, Gray Color, S/N G842PC1 from the custody of Platte River Networks and entered it into evidence as item 1B3 of the captioned investigation. The item was directly transported to the FBI Operational Technology Division (OTD) the same day. At 12:02 PM on October 20, 2015, SA [Redacted] picked up 1B3 from OTD where he discovered the original chain of custody was missing. SA [Redacted] transported 1B3 to the Washington Field Office and placed it into secure storage. This communication documents the

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

b3
b7E

b6
b7C

~~SECRET//NOFORN~~

Title: (U//~~FOUO~~) Chain of Custody for 1B3

Re: [redacted] 11/23/2015

b3
b7E

loss of the original chain of custody and the creation of a new chain of custody beginning with SA [redacted] on October 20, 2015.

b6
b7C

♦♦

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



OFFICIAL RECORD
Documents and signatures have digitally signed.
All signatures have been verified by a
certified FBI information system.

b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Evidence Entry

Event Title: (U) MIDYEAR EXAM

Date: 11/27/2015

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(U) ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

~~Reason: 1.4(c)~~

~~Derived From: Multiple
Sources~~

~~Declassify On: 20401231~~

Full Investigation Initiated: 07/10/2015

Collected By: Missing on Missing

Collected From: WILMER HALE
1875 PENNSYLVANIA AVE NW
WASHINGTON, District Of Columbia

Receipt Given?: No

Holding Office: WASHINGTON FIELD

Item Type	Description
1B Digital	(U) ONE (1) WESTERN DIGITAL MY PASSPORT ULTRA EXTERNAL HARD DRIVE WITH SERIAL NUMBER WXG1AA3M2130 Collected On: 11/25/2015 Seizing Individual: [REDACTED] Located By: [REDACTED] Location Area: 1875 PENNSYLVANIA AVE NW Specific Location: 1875 PENNSYLVANIA AVE NW Device Type: Portable Hard Drive Number of Devices Collected: 1

b6
b7C

(U) ~~SECRET//NOFORN~~

HRC-8653

[Redacted]

Serial 122

b3
b7E

~~SECRET//NOFORN~~

Title: (U) MIDYEAR EXAM

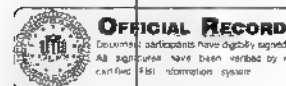
Re: [Redacted] 11/27/2015

b3
b7E

◆◆

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~



b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U//~~FOUO~~) Attorney Correspondence

Date: 12/04/2015

From: WASHINGTON FIELD

WF-CI13

Contact: [REDACTED]

Approved By: SSA [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(U) ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To document the submission of a FD-340 to the 1A sub-file section of the captioned case file.

~~Reason: 1.4(b)
Derived From: National
Security Information SCG
Declassify On: 20401231~~

Full Investigation Initiated: 07/10/2015

Enclosure(s): Enclosed are the following items:

1. (U//~~FOUO~~) 10/28/2015 Letter from DOJ to Wilmer Hale
2. (U//~~FOUO~~) 10/16/2015 Letter from Williams and Connolly to DOJ
3. (U//~~FOUO~~) 10/14/2015 Letter from Williams and Connolly to DOJ
4. (U//~~FOUO~~) 10/7/2015 Letter from Latham and Watkins to DOJ
5. (U//~~FOUO~~) 10/4/2015 Letter from DOJ to Williams and Connolly
6. (U//~~FOUO~~) 10/4/2015 Letter from DOJ to Williams and Connolly, and Latham and Watkins
7. (U//~~FOUO~~) 10/2/2015 Letter from Williams and Connolly to DOJ
8. (U//~~FOUO~~) 10/1/2015 Letter from Williams and Connolly to DOJ
9. (U//~~FOUO~~) Two 9/25/2015 Letters from Williams and Connolly to DOJ

Details:

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

HRC-8655

~~SECRET//NOFORN~~

Title: (U//~~FOUO~~) Attorney Correspondence

Re: [redacted] 12/04/2015

b3
b7E

(U//~~FOUO~~) This communication servers to document the submission of a
FD-340 (1A) to the 1A sub-file of the captioned case.

◆◆

~~SECRET//NOFORN~~

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

Serial 123

b3
b7E

Package:

1A43

Stored Location:

None

Summary:

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

2015-12-02

b6
b7C

Acquired On:

Attachment:

(U//~~FOUO~~) 10/28/2015
Letter from DOJ to
Wilmer Hale

HRC-8657

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

[REDACTED]
Serial 123

b3
b7E

Package:

1A43

Stored Location:

None

Summary:

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

[REDACTED]

b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) 10/16/2015
Letter from Williams and
Connolly to DOJ

HRC-8658

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

Serial 123

b3
b7E

Package:

1A43

Stored Location:

None

Summary:

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) 10/14/2015
Letter from Williams and
Connolly to DOJ

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

b3
b7E

Package:

Serial 123

Stored Location:

1A43

Summary:

None

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) 10/7/2015
Letter from Latham and
Watkins to DOJ

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

[REDACTED]
Serial 123

b3
b7E

Package:

1A43

Stored Location:

None

Summary:

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

[REDACTED]

b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) 10/4/2015
Letter from DOJ to
Williams and Connolly

HRC-8661

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

Serial 123

b3
b7E

Package:

1A43

Stored Location:

None

Summary:

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) 10/4/2015
Letter from DOJ to
Williams and Connolly,
and Latham and Watkins

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

b3
b7E

Package:

Serial 123

Stored Location:

1A43

Summary:

None

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) 10/2/2015
Letter from Williams and
Connolly to DOJ

HRC-8663

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

b3
b7E

Serial 123

Package:

1A43

Stored Location:

None

Summary:

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) 10/1/2015
Letter from Williams and
Connolly to DOJ

UNCLASSIFIED//~~FOUO~~

Physical 1A/1C Cover Sheet for Serial Export

Created From:

b3
b7E

Package:

Serial 123

Stored Location:

1A43

Summary:

None

(U//~~FOUO~~) Attorney
correspondence

Acquired By:

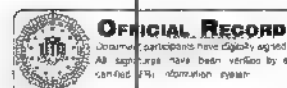
b6
b7C

Acquired On:

2015-12-02

Attachment:

(U//~~FOUO~~) Two 9/25/2015
Letters from Williams
and Connolly to DOJ



~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U//~~FOUO~~) Liaison Contacts

Date: 08/24/2016

From: WASHINGTON FIELD

WF-CI13

Contact: [REDACTED]

Approved By: SSA [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED]

(U)

~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To document liaison contacts encountered during investigation.

~~Reason: 1.4(b)~~

~~Derived From: FBI~~

~~NSISC-20090615~~

~~Declassify On: 20411231~~

Full Investigation Initiated: 07/10/2015

Details:

(U//~~FOUO~~) During the course of the captioned investigation, CI-13 had liaison contact with the departments and agencies below.

- Central Intelligence Agency
- Department of Defense
- Department of Energy
- Department of Homeland Security
- Department of Justice
- Department of State
- Department of Treasury
- Drug Enforcement Agency
- Executive Office of the President

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

HRC-8668

~~SECRET//NOFORN~~

Title: (U//~~FOUO~~) Liaison Contacts

Re: [REDACTED] 08/24/2016

b3
b7E

- National Aeronautics and Space Administration
- National Geospatial Agency
- National Reconnaissance Office
- National Security Agency
- National Security Council
- Office of Professional Management
- Office of the Director of National Intelligence
- United States Secret Service

◆◆

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1353814-0

Total Deleted Page(s) = 92

Page 2 ~ Referral/Consult;
Page 4 ~ Referral/Consult;
Page 5 ~ Referral/Consult;
Page 6 ~ Referral/Consult;
Page 7 ~ Referral/Consult;
Page 8 ~ Referral/Consult;
Page 9 ~ Referral/Consult;
Page 10 ~ Referral/Consult;
Page 11 ~ Referral/Consult;
Page 12 ~ Referral/Consult;
Page 13 ~ Referral/Consult;
Page 14 ~ Referral/Consult;
Page 15 ~ Referral/Consult;
Page 16 ~ Referral/Consult;
Page 17 ~ Referral/Consult;
Page 18 ~ Referral/Consult;
Page 19 ~ Referral/Consult;
Page 20 ~ Referral/Consult;
Page 21 ~ Referral/Consult;
Page 22 ~ Referral/Consult;
Page 23 ~ Referral/Consult;
Page 24 ~ Referral/Consult;
Page 25 ~ Referral/Consult;
Page 26 ~ Referral/Consult;
Page 27 ~ Referral/Consult;
Page 28 ~ Referral/Consult;
Page 29 ~ Referral/Consult;
Page 30 ~ Referral/Consult;
Page 31 ~ Referral/Consult;
Page 32 ~ Referral/Consult;
Page 33 ~ Referral/Consult;
Page 34 ~ Referral/Consult;
Page 35 ~ Referral/Consult;
Page 36 ~ Referral/Consult;
Page 37 ~ Referral/Consult;
Page 38 ~ Referral/Consult;
Page 39 ~ Referral/Consult;
Page 40 ~ Referral/Consult;
Page 41 ~ Referral/Consult;
Page 42 ~ Referral/Consult;
Page 43 ~ Referral/Consult;
Page 44 ~ Referral/Consult;
Page 45 ~ Referral/Consult;
Page 46 ~ Referral/Consult;
Page 47 ~ Referral/Consult;
Page 48 ~ Referral/Consult;
Page 49 ~ Referral/Consult;
Page 50 ~ Referral/Consult;

Page 51 ~ Referral/Consult;
Page 52 ~ Referral/Consult;
Page 53 ~ Referral/Consult;
Page 54 ~ Referral/Consult;
Page 55 ~ Referral/Consult;
Page 56 ~ Referral/Consult;
Page 57 ~ Referral/Consult;
Page 58 ~ Referral/Consult;
Page 59 ~ Referral/Consult;
Page 60 ~ Referral/Consult;
Page 61 ~ Referral/Consult;
Page 62 ~ Referral/Consult;
Page 63 ~ Referral/Consult;
Page 64 ~ Referral/Consult;
Page 65 ~ Referral/Consult;
Page 66 ~ Referral/Consult;
Page 67 ~ Referral/Consult;
Page 68 ~ Referral/Consult;
Page 69 ~ Referral/Consult;
Page 70 ~ Referral/Consult;
Page 71 ~ Referral/Consult;
Page 72 ~ Referral/Consult;
Page 73 ~ Referral/Consult;
Page 74 ~ Referral/Consult;
Page 75 ~ Referral/Consult;
Page 76 ~ Referral/Consult;
Page 77 ~ Referral/Consult;
Page 78 ~ Referral/Consult;
Page 79 ~ Referral/Consult;
Page 80 ~ Referral/Consult;
Page 81 ~ Referral/Consult;
Page 82 ~ Referral/Consult;
Page 83 ~ Referral/Consult;
Page 84 ~ Referral/Consult;
Page 85 ~ Referral/Consult;
Page 86 ~ Referral/Consult;
Page 87 ~ Referral/Consult;
Page 88 ~ Referral/Consult;
Page 89 ~ Referral/Consult;
Page 90 ~ Referral/Consult;
Page 91 ~ Referral/Consult;
Page 92 ~ Referral/Consult;
Page 93 ~ Referral/Consult;
Page 94 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXX

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1353814-0

Total Deleted Page(s) = 90

Page 6 ~ b1; b3; b6; b7C; b7E;
Page 7 ~ b1; b3; b6; b7C; b7E;
Page 8 ~ b1; b3; b6; b7C; b7E;
Page 9 ~ b1; b3; b7E;
Page 13 ~ b1; b3; b6; b7C; b7E;
Page 14 ~ b1; b3; b6; b7C; b7E;
Page 15 ~ b1; b3; b6; b7C; b7E;
Page 16 ~ b1; b3; b6; b7C; b7E;
Page 20 ~ b1; b3; b6; b7C; b7E;
Page 21 ~ b1; b3; b6; b7C; b7E;
Page 25 ~ Referral/Consult;
Page 26 ~ Referral/Consult;
Page 27 ~ Referral/Consult;
Page 28 ~ Referral/Consult;
Page 29 ~ Referral/Consult;
Page 30 ~ Referral/Consult;
Page 43 ~ Referral/Consult;
Page 44 ~ Referral/Consult;
Page 45 ~ Referral/Consult;
Page 46 ~ Referral/Consult;
Page 47 ~ Referral/Consult;
Page 48 ~ Referral/Consult;
Page 49 ~ Referral/Consult;
Page 56 ~ Referral/Consult;
Page 57 ~ Referral/Consult;
Page 58 ~ Referral/Consult;
Page 71 ~ Duplicate;
Page 72 ~ Duplicate;
Page 73 ~ Duplicate;
Page 77 ~ Referral/Consult;
Page 78 ~ Referral/Consult;
Page 79 ~ Referral/Consult;
Page 80 ~ Referral/Consult;
Page 81 ~ Referral/Consult;
Page 82 ~ Referral/Consult;
Page 83 ~ Referral/Consult;
Page 84 ~ Referral/Consult;
Page 85 ~ Referral/Consult;
Page 86 ~ Referral/Consult;
Page 87 ~ Referral/Consult;
Page 88 ~ Referral/Consult;
Page 89 ~ Referral/Consult;
Page 94 ~ b1; b3; b6; b7A; b7C; b7E;
Page 95 ~ b1; b3; b6; b7A; b7C; b7E;
Page 112 ~ b1; b3; b7E;
Page 125 ~ Duplicate;
Page 126 ~ Duplicate;
Page 127 ~ Duplicate;

Page 148 ~ Duplicate;
Page 149 ~ Duplicate;
Page 150 ~ Duplicate;
Page 151 ~ Duplicate;
Page 161 ~ b1; b3; b7E;
Page 163 ~ Referral/Consult;
Page 164 ~ Referral/Consult;
Page 165 ~ Referral/Consult;
Page 166 ~ Referral/Consult;
Page 167 ~ Referral/Consult;
Page 170 ~ b7E;
Page 171 ~ b7E;
Page 172 ~ b6; b7C; b7E;
Page 173 ~ b7E;
Page 175 ~ b3; b6; b7C; b7E;
Page 176 ~ b7E;
Page 177 ~ b6; b7C; b7E;
Page 178 ~ b7E;
Page 179 ~ b7E;
Page 180 ~ b7E;
Page 190 ~ Referral/Consult;
Page 191 ~ Referral/Consult;
Page 192 ~ Referral/Consult;
Page 193 ~ Referral/Consult;
Page 194 ~ Referral/Consult;
Page 195 ~ Referral/Consult;
Page 196 ~ Referral/Consult;
Page 197 ~ Referral/Consult;
Page 198 ~ Referral/Consult;
Page 199 ~ Referral/Consult;
Page 200 ~ Referral/Consult;
Page 201 ~ Referral/Consult;
Page 202 ~ Referral/Consult;
Page 203 ~ Referral/Consult;
Page 204 ~ Referral/Consult;
Page 205 ~ Referral/Consult;
Page 206 ~ Referral/Consult;
Page 207 ~ Referral/Consult;
Page 208 ~ Referral/Consult;
Page 209 ~ Referral/Consult;
Page 210 ~ Referral/Consult;
Page 211 ~ Referral/Consult;

XXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXX

2/24/16
Serial 2

~~SECRET~~

b6
b7c

~~SECRET~~

HRC-8762

~~SECRET//NOFORN~~ [redacted] (S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Precedence: ROUTINE

Date: 02/01/2016

To: Washington Field

From: Washington Field

CI-13

Contact: [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

(U) **Case ID #:** ~~(S//NF)~~ [redacted] CYBER-2

b3
b7E

(U) **Title:** ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

(U) **Synopsis:** ~~(S//NF)~~ Summary of [redacted] searches related to clintonemail.com and presidentclinton.com.

b7E

~~Classified By: C21W96B63
Derived From: FBI NSIC dated 20130301
Declassify On: 20410201~~

b1
(S) b3
b7E

~~SECRET//NOFORN~~ [redacted] (S)

b1
b3
b7E

~~SECRET~~ / ~~NOFORN~~

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

(S) b1
b3
b7E

Details: (S//NF) [redacted] This EC summarizes research conducted by the writer in September 2015 in [redacted] based on searches for the domain names 'clintonemail.com' and 'presidentclinton.com'. The results of these searches showed the following:

b1
b3
b7E

(S) b1
b3
b7E

(U//FOUO) These events are described in detail below.

~~SECRET~~ / ~~NOFORN~~

(S)

b1
b3
b7E

3/3/16
Serial 3

~~SECRET~~

b6
b7C

HRC-8769

~~SECRET~~

~~SECRET~~ / ~~NOFORN~~ []

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 2/29/2016

To: Washington Field

From: Washington Field

CI-13

Contact: SA []

b6
b7C

Approved By: []

Drafted By: []

(U) **Case ID #:** (S) [] -CYBER - 3

b3
b7E

(U) **Title:** (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: []

b1
b3
b6
b7C
b7E

~~Classified By: J91J44T84~~
~~Derived From: FBI NSIC dated 20130301~~
~~Declassify On: 20410229~~

b1
b3
b7E

~~SECRET~~ / ~~NOFORN~~ []

b1
b3
b7E

~~SECRET~~ / ~~NOFORN~~ [redacted]

(S)

FEDERAL BUREAU OF INVESTIGATION

b1
b3
b7E

b1
(S) b3
b7E

Details: (~~S~~/~~NF~~) This communication documents investigative analysis performed on digital evidence that was obtained for the email account of [redacted] The subscriber of that account has been identified as [redacted]

b1
b3
b6
b7C
b7E

(S)

~~SECRET~~ / ~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

3/7/16
Serial 4

~~SECRET~~

b6
b7c

HRC 8776

~~SECRET~~

~~SECRET~~/NOFORN [redacted]

(S)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/04/2016

To: Washington Field

From: Washington Field

CI-13

Contact: SA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

(U) **Case ID #:** (S) [redacted] -CYBER- 4

b3
b7E

(U) **Title:** (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: [redacted]

b1
b3
b6
b7C
b7E

Classified By: J91J44T84
Derived From: FBI NSIC dated 20130301
Declassify On: 20410304

Reference: [redacted] -CYBER, Serial 3

b3
b7E

(S)

b1
b3
b7E

~~SECRET~~/NOFORN [redacted]

(S)

b1
b3
b7E

~~SECRET~~ / ~~NOFORN~~

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

(S) b1
b3
b7E

Details:

(S) b1
b3
b7E

~~(S/NO)~~ This communication documents investigative analysis performed on digital evidence that was obtained for the GMAIL account of [REDACTED] The subscriber of that account has been identified as [REDACTED]

(S) b1
b3
b6
b7C
b7E

~~SECRET~~ / ~~NOFORN~~

(S)

b1
b3
b7E

3/24/86
Serial 5

~~SECRET~~

b6
b7c

HRC 8/81

~~SECRET~~

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Precedence: ROUTINE

Date: 3/9/2016

To: Washington Field

From: Washington Field

CI-13

Contact: [REDACTED]

b6
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** ~~(S)~~ [REDACTED]-CYBER -5

b3
b7E

(U) **Title:** ~~(S)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To memorialize Intelligence Bulletin
authored by IA [REDACTED] on 29 October 2016.

b6
b7C

~~Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410223~~

(U) **Details:** ~~(S//NF)~~ Cyber Division IA [REDACTED] supported
captioned investigation from 9 September to 30 October 2016.
During IA [REDACTED] tenure, he conducted research on
approximately [REDACTED] email addresses found in the To:, From:, Cc:,
or Bcc: portions of emails sent to any of Hillary Rodham
Clinton's (HRC) electronic accounts. The approximately [REDACTED] email
addresses were found in the .pst file provided to the FBI in
August 2015 by Williams & Connolly, HRC's attorneys.

b6
b7C
b7E

~~(S//NF)~~ IA [REDACTED] conducted bulk search of identified
email accounts in [REDACTED]

b1
b3
b6
b7C
b7E

(S)

(U//~~FOUO~~) An electronic copy of the aforementioned
intelligence product, search results conducted in FBI databases

~~SECRET//NOFORN~~

HRC-8782

~~SECRET~~ // NOFORN

FEDERAL BUREAU OF INVESTIGATION

by IA and iC3 results are enclosed in a 1A envelope for the file.

b6
b7C

♦♦

~~SECRET~~ // NOFORN

HRC-8783

3/2/16
Serial 7

~~SECRET~~

b6
b7c

HRC 8/90

~~SECRET~~

~~SECRET//NOFORN~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/08/2016

To: Washington Field

From: Washington Field

CI-13

Contact: SA [REDACTED]

b6
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** (S) [REDACTED] -CYBER -7

b3
b7E

(U) **Title:** (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) Documents analysis of suspicious logon attempts to the APPLE ICLOUD account associated with hdr22@clintonemail.com.

Classified By: J91J44T84
Derived From: FBI NSIC dated 20130301
Declassify On: 20410308

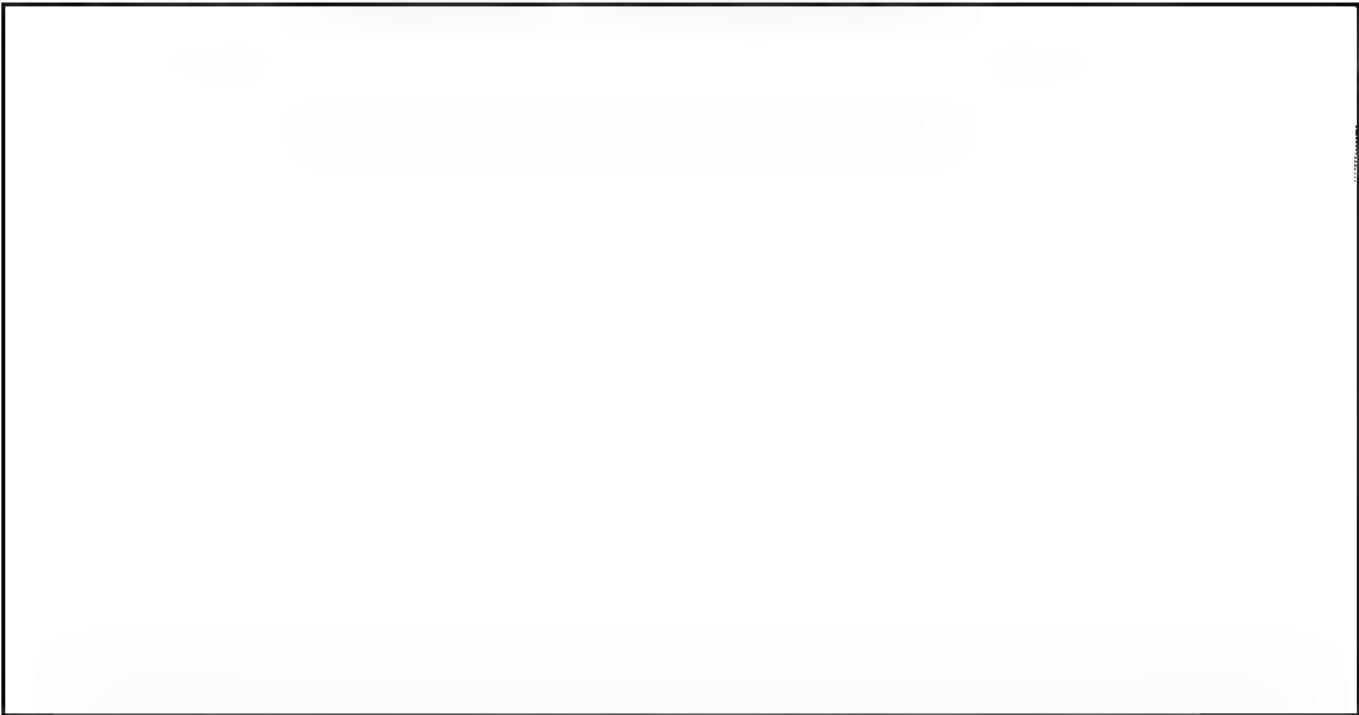
b1
b3
b7E

(S)

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION



(S)

b1
b3
b7E

Details: (U//~~FOUO~~) Writer conducted an analysis of logon attempts to the APPLE ICLOUD account associated with the email address of hdr22@clintonemail.com. Records were received from the APPLE internet service provider which identified 126 logon attempts made to that account, between the dates of 03/03/2015 and 12/13/2015. Of those attempts, 121 were made using the APPLE IFORGOT feature, and 5 were made using the MYAPPLEID feature.

(U//~~FOUO~~) The table on the following page depicts:



b7E



~~SECRET//NOFORN~~

~~SECRET~~ // ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~)

b6
b7C
b7E

(U//~~FOUO~~) Writer then conducted logical investigative follow-up on each of the above addresses. The following is a summary of the pertinent findings.

(U//~~FOUO~~)

b3
b7E

(U//~~FOUO~~) This investigation has identified the subscriber of IP addresses [redacted] as being

b3
b6
b7C
b7E

[redacted] A total of [redacted] login attempts were conducted from [redacted] IP addresses [redacted]

(U//~~FOUO~~)

b3
b7E

~~SECRET~~ // ~~NOFORN~~

~~SECRET~~/NOFORN

FEDERAL BUREAU OF INVESTIGATION

(U//FOUO) At this time, no additional information has been identified to explain [REDACTED]

b3
b7E

[REDACTED] Of significance is that the [REDACTED] login attempts began on 03/03/2016, which occurred a day after the New York Times release of Clinton's use of a personal email system. Writer recommends that Agents conduct an interview with [REDACTED] in attempt to determine further information about the login attempts to the ICLOUD hdr22@clintonemail.com account.

(U//FOUO) [REDACTED]

(U//FOUO) [REDACTED]

[REDACTED] is the subject of FBI investigation [REDACTED]

b3
b6
b7A
b7C
b7E

[REDACTED] was also used for the attempted unauthorized access of [REDACTED] additional APPLE ICLOUD accounts. The majority of the targeted victims appeared to be celebrity figures, politicians, and/or corporate executives. San Francisco was able to positively attribute the unauthorized logins to [REDACTED]

(U//FOUO) [REDACTED]

b6
b7A
b7C
b7E

(U//FOUO) During [REDACTED]

b6
b7A
b7C
b7E

~~SECRET~~/NOFORN

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

[REDACTED]

b6
b7A
b7C
b7E

(U//~~FOUO~~) Investigation in this matter has determined that [REDACTED] was likely responsible for [REDACTED] logon attempts to the hdr22@clintonemail.com ICLOUD account. Those attempts originated from [REDACTED]

[REDACTED]

b6
b7C
b7E

[REDACTED] admitted attempting to logging into ICLOUD accounts from [REDACTED]. Lastly, [REDACTED] was identified in the San Francisco investigation as also being [REDACTED]

[REDACTED]

(U//~~FOUO~~) Additionally, [REDACTED]

[REDACTED] is referenced in [REDACTED]. A review of that investigation identified that

[REDACTED]

b3
b6
b7A
b7C
b7E

(U//~~FOUO~~) In support of this investigation, San Francisco provided writer with [REDACTED]

[REDACTED] A review of that evidence identified [REDACTED]

[REDACTED]

b6
b7A
b7C
b7E

(U//~~FOUO~~) Given that [REDACTED] admitted conducting unauthorized access attempts to ICLOUD accounts [REDACTED]

[REDACTED] were also obtained for [REDACTED]. In reviewing those records, writer assesses that [REDACTED] is likely responsible for the logon attempt [REDACTED]

[REDACTED]

b6
b7C
b7E

[REDACTED] However, no additional evidence was identified to corroborate [REDACTED]

~~SECRET//NOFORN~~

~~SECRET~~ / ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) UNKNOWN ACTORS

[Redacted]

(S)

b1
b3
b7A
b7E

(U//~~FOUO~~)

[Redacted]

b3
b6
b7C
b7E

(U//~~FOUO~~) Attempts to find additional identifying information for the actors conducting login attempts from foreign IP addresses

[Redacted]

were all met with negative results.

b6
b7C

(U//~~FOUO~~) ENCLOSURES

(U//~~FOUO~~) Enclosed for the file in a 1A envelope is one compact disk containing:

[Redacted]

b3
b6
b7C
b7E

♦♦

~~SECRET~~ / ~~NOFORN~~

3/22/16
Serial 8

~~SECRET~~

b6
b7c

HRC-8797

~~SECRET~~

~~SECRET//NOFORN~~ [redacted] (S)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 3/21/2016

To: Washington Field

From: Washington Field

CI-13

Contact: IA [redacted]

b6
b7C

Approved By: [redacted]

Drafted By: [redacted]

(U) **Case ID #:** ~~(S)~~ [redacted] -CYBER -8

b3
b7E

(U) **Title:** ~~(S)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

(U) **Synopsis:** ~~(S//NF)~~ To document [redacted] search results of email addresses found in confirmed classified messages and/or belonging to individuals part of Hillary Rodham Clinton's close circle.

b7E

~~Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410223~~

Details: (U//~~FOUO~~) Through the course of captioned investigation, numerous email addresses found in confirmed classified messages and/or belonging to individuals part of Hillary Rodham Clinton's (HRC) close circle have been identified. Writer conducted [redacted] queries on all facilities between 12 and 21 February 2016; results are as follow.

b7E

(U//~~FOUO~~) Email Addresses Found in Confirmed Classified

(U//~~FOUO~~) On 12 January 2016, ITSpec [redacted] compiled a histogram of email addresses found in confirmed classified messages up to that date. The list was captured in a Excel workbook [redacted] which writer edited in order to capture additional information, as well as [redacted] search results.

b6
b7C
b7E

(U//~~FOUO~~) [redacted]

b7E

~~SECRET//NOFORN~~ [redacted] (S)

b1
b3
b7E

HRC-8798

~~SECRET~~ / ~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

b7E

(U//~~FOUO~~) A printout of a Microsoft Excel worksheet [redacted] along with [redacted]

[redacted] results, is enclosed in a 1A envelope for the file.

b7E

(U) [redacted] Queries

(S//~~NF~~) Writer conducted [redacted] queries on [redacted]

b1
b3
b6
b7C
b7E

(S)

(U) [redacted] Queries

b7E

(S//~~NF~~) Writer conducted [redacted] queries on [redacted]

b7E

(U) [redacted] on Sunday, 21 February 2016. [redacted]

[redacted] There was no indication that the facilities of interest were themselves compromised.

b1
b3
(S) b7E

~~SECRET~~ / ~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8799

~~SECRET//NOFORN~~ [redacted]

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

[redacted] (S)

b1
b3
b7E

(U)

(S//NF) It is unknown whether [redacted]
[redacted] a coincidence or an attempt to
impersonate HRC's hdr22@clintonemail.com account. To the FBI's
knowledge, [redacted]

b7E

(U//FOUO) A printout of a Microsoft Excel worksheet
[redacted] along with [redacted]
[redacted] results, is enclosed in a 1A envelope for the file.

b7E

(U//FOUO) [redacted] Belonging to HRC's Close Circle

(U)

(S//NF) Prior to writer's arrival to CI-13, Cyber
Division IA [redacted] supported captioned investigation from
9 September to 30 October 2016. IA [redacted] perused the data set
of approximately 30,000 emails obtained from Williams &
Connolly, and identified about [redacted] belonging to
individuals part of HRC's close circle [redacted]

b6
b7C
b7E

(S//NF) Writer's Note: IA [redacted]
search results were captured in an Intelligence Bulletin titled [redacted]

b1
b3
b6
b7C
b7E

[redacted] research and intelligence product
are captured in a preceding MIDYEAR EXAM serial.

(U//FOUO) Writer conducted [redacted]

[redacted] (S)

b1
b3
b6
b7C
b7E

~~SECRET//NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8800

~~SECRET~~//~~NOFORN~~ [redacted]

(S)

FEDERAL BUREAU OF INVESTIGATION

b1
b3
b7E

(S)

b1
b3
b7E

(U//~~FOUO~~) A printout of a Microsoft Excel worksheet listing the [redacted] along with [redacted] results, is enclosed in a 1A envelope for the file.

b7E

(U//~~FOUO~~) Writer further created two additional worksheets to compare [redacted] with the [redacted] associated with HRC's close circle in order to identify overlaps in both lists and ensure all accounts had been properly accounted for. Both worksheets are enclosed in a 1A envelope for the file.

b7E

♦♦

~~SECRET~~//~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8801

3/24/16
Serial 10

b6
b7C

HRC-8809
r

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/21/2016

To: Washington Field

From: Washington Field

CI-13

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** ~~(S//NF)~~ [REDACTED] -CYBER -10

(U) **Title:** ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) Analysis performed by TOU on referenced evidence item to check for common artifacts of cyber intrusion activity, malware, and other forms of unauthorized access.

~~Classified By: C21W96B63
Derived From: FBI-NSIC dated 20130301
Declassify On: 20410321~~

Details: (U//~~FOUO~~) At the request of Counterintelligence Division (CD) and WFO Squad CI-13, the Cyber Division (CyD) Technical Operations Unit (TOU) performed an analysis of the forensic image of the following evidence item to check for the presence of malware and/or other indicators of compromise (IOCs):

- Case ID: [REDACTED]
- Lab #: 150806250
- Specimen: DEHQ55
- Item: QHQ1_1
- Description: Lexar Micron 16GB LJDTT16G-000-1001DA

(U//~~FOUO~~) TOU performed scans to identify malicious attachments within an email archive found on the forensic image of the referenced USB device. Several malicious attachments were identified among the [REDACTED] email messages [REDACTED]. Malware analysis was performed on these samples,

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

b3
b7E

b7E

~~SECRET~~ // ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

and based on this analysis TOU is categorizing these into two separate incidents.

(U//~~FOUO~~) The first incident pertains to emails associated with a widespread phishing attack referenced in [REDACTED]

b3
b7A
b7E

[REDACTED] associated with this campaign. No further analysis was performed on these samples since the samples matched those in the report referenced above.

(U//~~FOUO~~) The second incident pertains to a suspicious email received on Nov 6, 2009 from [REDACTED] titled [REDACTED]. The email contained a malicious PDF that was determined to be a dropper for a common Remote Access Tool (RAT) called Poison Ivy.

b6
b7C
b7E

(U//~~FOUO~~) Detailed analysis and indicators are provided in the attached report. Also attached is an open source report found at <https://raw.githubusercontent.com/fireeye/pivy-report/master/PIVY-Appendix.pdf>, which depicts the malware from the second incident in the context of a broader set of APT activity. These findings will be provided to the CyD analysis cell assisting with this matter for logical investigative follow-up [REDACTED]

b7E

♦♦

~~SECRET~~ // ~~NOFORN~~

7/21/16
Serial 4

b6
b7c

HRC-8812

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/21/2016

To: Washington Field

From: Washington Field

CI-13

Contact: [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) Case ID #: ~~(S//NF)~~ [REDACTED] -CYBER -((

(U) Title: ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) Analysis performed by TOU on referenced evidence item to check for common artifacts of cyber intrusion activity, malware, and other forms of unauthorized access.

~~Classified By: C21W96B63~~
~~Derived From: FBI NSIC dated 20130301~~
~~Declassify On: 20410321~~

(U) Details: ~~(S//NF)~~ At the request of Counterintelligence Division (CD) and WFO Squad CI-13, the Cyber Division (CyD) Technical Operations Unit (TOU) performed an analysis of the forensic image of the following evidence item to check for the presence of malware and/or other indicators of compromise (IOCs):

- Case ID: [REDACTED]
- Lab #: 150806250
- Specimen: DEHQ55
- Item: QHQ2_1
- Description: Toshiba Laptop from Williams & Connolly LLP

(U//~~FOUO~~) A detailed intrusion analysis of the forensic image of the laptop [REDACTED] was performed. No indications were found that an attacker may have gained unauthorized access to the machine. The machine was in service during the period of March 14, 2012 to August 6, 2015 on Williams & Connolly

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

b3
b7E

b7E

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

LLP's network. The machine was used infrequently over the 3-year period by [] unique user accounts.

b7E

(U//~~FOUO~~) The machine was used to review emails in preparation for delivery to the FBI. Those emails are contained within an archive file [] located on the desktop of the user account []. This archive was analyzed for malware, which is documented in an adjoining report in the case file for [] Lab #: 150806250 Specimen: DEHQ55 Item: QHQ1_1.

b3
b7E

(U//~~FOUO~~) Detailed analysis of this item is documented in the attached report. Also attached are the supporting [] reports. These findings will be provided to the CyD analysis cell assisting with this matter for logical investigative follow-up.

b7E

♦♦

~~SECRET//NOFORN~~

3/24/16
Section 13

b6
b7c

HRC 8818

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/22/2016

To: Washington Field

From: Washington Field

CI-13

Contact: SA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) Case ID #: (S) [REDACTED] CYBER-13

(U) Title: (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

(U) Synopsis: (S//NF) [REDACTED] searches conducted by NCIJTF.

~~Classified By: J91J44T84~~

~~Derived From: FBI NSIC dated 20130301~~

~~Declassify On: 20410322~~

(U) Details: (S//NF) In furtherance of this investigation, the FBI conducted investigative queries for facilities of interest in this matter, within the [REDACTED] Those queries were conducted by [REDACTED] currently assigned to the FBI's NCIJTF in Chantilly, Virginia.

(U) (S//NF) Enclosed for the file in a physical 1A envelope is one compact disk, containing the results of the [REDACTED] queries that were conducted for this investigation.

♦♦

~~SECRET//NOFORN~~

HRC-8819

3/24/16
Serial 15

~~SECRET~~

b6
b7c

HRC 8820

~~SECRET~~

~~SECRET~~ // ~~NOFORN~~ [redacted] (S)

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1

b3

b7E

Precedence: ROUTINE

Date: 3/22/2016

To: Washington Field

From: Washington Field

CI-13

Contact: IA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (S) [redacted]

-CYBER -15

Title: (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (S) // (NF) To document research and analysis conducted on identified email accounts associated with Hillary Rodham Clinton (HRC) and any information related to the clintonemail.com domain.

~~Classified By: F36M12K15~~
~~Derived From: FBI NSIC dated 20130301~~
~~Declassify On: 20410223~~

(S)

b1
b3
b7E

~~SECRET~~ // ~~NOFORN~~ [redacted] (S)

HRC-8821

~~SECRET~~ // ~~NOFORN~~ [] (S)

FEDERAL BUREAU OF INVESTIGATION

(S)
b1
b3
b7E

(U) Details: (~~S~~/~~NF~~) Investigation to date has led to the identification of [] email addresses associated with HRC. Writer queried Sentinel, [] and [] for information related to the accounts. []

b7E

[] Positive results are noted below and further detailed in a Microsoft Excel spreadsheet enclosed on a disc in a 1A envelope for the file.

(U) (~~S~~/~~NF~~) Based on a list of identified email addresses obtained from various sources, queries were conducted on the following accounts:

1	ClintonHR@state.gov
2	[]
3	
4	
5	
6	
7	
8	hdr22@clintonemail.com
9	hdr29@clintonemail.com
10	hdr29@hrcoffice.com
11	[]
12	
13	hrl5@att.blackberry.net
14	hrl5@mycingular.blackberry.net
15	[]
16	
	hrcarchive@clintonemail.com
	hrcarchive@presidentclinton.com

b6
b7C
b7E~~SECRET~~ // ~~NOFORN~~ [] (S)b1
b3
b7E
HRC-8822

~~SECRET~~ // ~~NOFORN~~ [redacted] (S)

FEDERAL BUREAU OF INVESTIGATION

17 hrod17@clintonemail.com

b6
b7C
b7E

(U//~~FOUO~~) ClintonHR@state.gov

(U//~~FOUO~~) Sentinel Queries

[redacted]

(S)

b1
b3
b7A
b7E

(U) ~~(S//NF)~~ Per [redacted] following a discussion with a Confidential Human Source (CHS), FBI Tampa

b3
b7D
b7E

[redacted] Per serial 18 of the same investigation, parsing of the data revealed [redacted] No additional information related to the targeting of ClintonHR@state.gov was identified.

(U) ~~(S//NF)~~ Per [redacted]

b3
b7A
b7E

[redacted] No additional information related to this incident was identified.

(U) ~~(S//NF)~~ Per [redacted]

b3
b7A
b7E

[redacted] No additional information was gleaned from the referenced case file.

~~SECRET~~ // ~~NOFORN~~ [redacted] (S)

b1
b3
b7E

HRC-8823

~~SECRET~~//~~NOFORN~~ [redacted]

(S)

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) [redacted] Queries

(S)

b1
b3
b7E

(U) [redacted] Queries

(S)

b1
b3
b7E

(U//~~FOUO~~) HDR22@clintonemail.com

(U//~~FOUO~~) Sentinel Queries

(U) ~~(S//NF)~~ A search of HDR22@clintonemail.com in Sentinel revealed the account was the target of various unauthorized iCloud login attempts by [redacted]. Analysis of [redacted] highlighted approximately [redacted] attempts between 15 May and 30 June 2015. Per [redacted]

b3
b6
b7A
b7C
b7E

[redacted] stated that HDR22@clintonemail.com had only [redacted]. Additional analysis related to [redacted] attempt to gain unauthorized access to the associated iCloud account is documented in MIDYEAR EXAM, Cyber sub-folder, serial 7.

(U) ~~(S//NF)~~ While reviewing [redacted] related to the aforementioned FBI San Francisco investigation, writer also identified [redacted]

b6
b7A
b7C
b7E

(U) ~~(S//NF)~~ Additional Sentinel results referenced open source articles from 2015 that mentioned HDR22@clintonemail.com. No valuable intelligence was gleaned from the articles. [Reference: Various [redacted] serials]

b3
b7E

~~SECRET~~//~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8824

~~SECRET~~//~~NOFORN~~

(S)

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) [redacted] Queries

b1
b3
b7E

b1
b3
b6
b7C
b7E

(S)

(U) ~~(S//NF)~~ [redacted] results for HDR22@clintonemail.com are enclosed on a disc in a 1A envelope for the file.

b7E

(U) Additional Research

(U) ~~(S//NF)~~ Writer was alerted by the MIDYEAR EXAM Review Team on 21 March 2015 of a likely spear-phishing incident targeting HDR22@clintonemail.com [redacted] on 5 June 2011. The email was sent from [redacted] and was purportedly a DHL delivery notification, which enclosed an attachment titled "DHL mail.zip." HDR forwarded the email to Human ABEDIN (huma@clintonemail.com) asking if she knew what the email was about, also stating she deleted the message upon receipt. A search for the sender address in Sentinel yielded negative results.

b7E

(U//~~FOUO~~) HR15@mycingular.blackberry.net

(U//~~FOUO~~) Sentinel Queries

(U) ~~(S//NF)~~ Per [redacted] dated 10 November 2015, [redacted]
[redacted]
[redacted] Based on [redacted]
[redacted] and attached to referenced serial in [redacted]

b3
b6
b7A
b7C
b7E

(U//~~FOUO~~) HROD17@clintonemail.com

(U//~~FOUO~~) Sentinel Queries

(U) ~~(S//NF)~~ A search of HROD17@clintonemail.com in Sentinel revealed [redacted]

b6
b7C
b7E

~~SECRET~~//~~NOFORN~~

(S)

b1
b3
b7E

HRC-8825

~~SECRET~~//NOFORN [redacted]

(U)

FEDERAL BUREAU OF INVESTIGATION

b1
(U) b3
b6
b7C
b7E

(U) Additional Research

(U) ~~(S//NF)~~ Per research conducted by IA [redacted] during his TDY (9 September to 30 October 2015) to support captioned investigation. HROD17@clintonemail.com was the

b1
b3
b6
(S) b7C
b7E

(S) [redacted] (S)

[redacted] According to IA research, [redacted]

[redacted] In an open source article referenced by IA [redacted] the malicious attachment(s), if opened, would have compromised the host and sent information to at least three computers overseas, including one in Russia. According to the same open source article, a spokesman for HRC said there was no evidence of a breach.

(U//~~FOUO~~) The phishing event was summarized by IA [redacted] in a separate report and is enclosed on a disc in a 1A envelope for the case file.

b6
b7C

(U//~~FOUO~~) ClintonEmail.com Domain

(U) ~~(S//NF)~~ In addition to queries conducted on known email accounts belonging to HRC, writer also queried FBI systems for any additional information related to the clintonemail.com domain, filtering for [redacted] information only. The following was gleaned from queries conducted in Sentinel and [redacted]

b7E

(U//~~FOUO~~) Sentinel Queries

(U) ~~(S//NF)~~ Queries on the clintonemail.com domain yielded approximately [redacted] results, some of which are documented above. One result of interest not previously captured details reporting in which a CHS states [redacted]

b6
b7A
b7C
b7D
b7E

[redacted] It is unknown what, if anything, prompted the CHS to identify and report [redacted] No

~~SECRET~~//NOFORN [redacted]

(U)

b1
b3
b7E

HRC-8826

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

FEDERAL BUREAU OF INVESTIGATION

further information related to the event was found in Sentinel holdings. [Reference: [redacted]]

(U//~~FOUO~~) Remaining Sentinel hits referenced open source articles in which the domain was mentioned, warranting no further action. Additional open source research on the domain and logical pivoting is detailed in MIDYEAR EXAM, Main case file, serial 141.

(U//~~FOUO~~) [redacted] Queries

[Large redacted area]

(U) (~~S~~//~~NF~~) In September 2015, SSA [redacted] (CyD/TOU) conducted [redacted] searches on the clintonemail.com and presidentclinton.com domains. His findings are serialized in MIDYEAR EXAM, Cyber sub-folder, serial 2.

(U) Additional Queries

(U) (~~S~~//~~NF~~) On or about October 2015, the MIDYEAR EXAM Investigative Team submitted a list of email addresses associated with HRC. Targeter [redacted], NCIJTF Office of Analysis and Assessments, conducted a [redacted] search on [redacted] which yielded negative results. Targeter [redacted] report [redacted] is enclosed on a disc in a 1A envelope for the case file.

♦♦

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

HRC-8827

3/14/14
Serial 16

b6
b7c

HRC-8828

to James
7/11/2006

b6
b7c

HRC 8832

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 03/23/2016

To: Washington Field

From: Washington Field

WF CART

Contact:

Approved By:

Drafted By:

(U) Case ID #: ~~(S//NF)~~ [REDACTED] -CYBER -17

(U) Title: ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

(U) Synopsis: ~~(S//NF)~~ Final technical analysis report from IAU

~~Classified By: F41M65K83
Derived From: FBI NSIC dated 20130301
Declassify On: 20411231~~

(U) Details: ~~(S//NF)~~ On October 20, 2015, Information Technology Specialist/Forensic Examiner [REDACTED] of the Washington Field Office Computer Analysis Response Team (CART) requested the assistance of the Operational Technology Division (OTD) Investigative Analysis Unit (IAU) in support of the case [REDACTED]. The details of the request are documented in Serial-3 in the [REDACTED] CART sub-file.

(U) evidence: ~~(S//NF)~~ IAU conducted an analysis of the following digital

[REDACTED]

~~SECRET//NOFORN~~

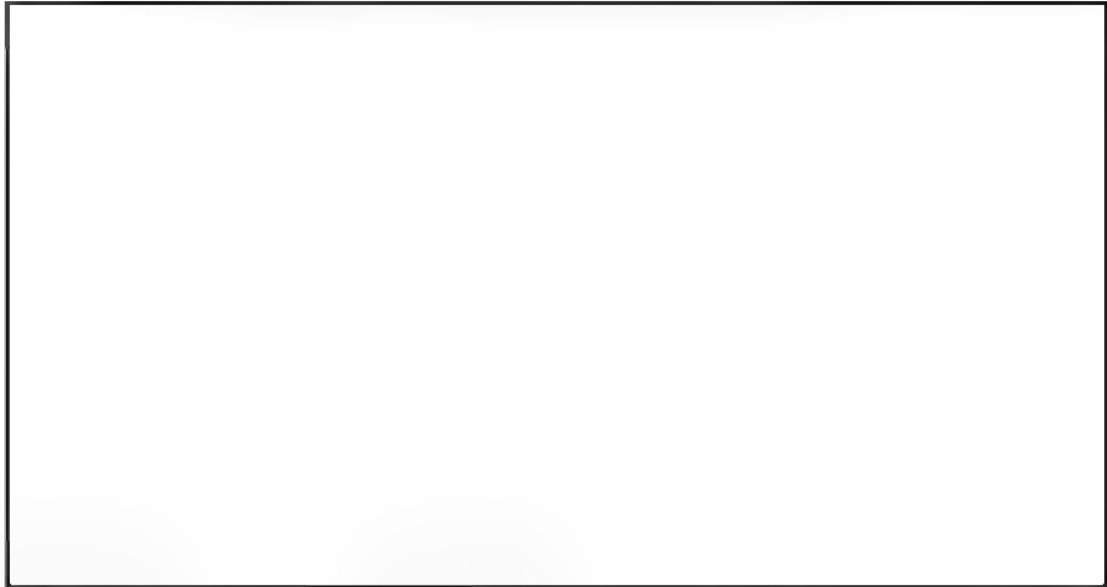
b3
b6
b7C
b7E

b3
b6
b7C
b7E

b7E

~~SECRET~~ // ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION



b7E

(U) ~~(S//NF)~~ A report dated February 10, 2016 containing the results of the analysis of digital evidence for intrusion-related activities was provided to ITS/FE [redacted] by IT Specialists [redacted] and [redacted] of the Investigative Analysis Unit. A copy of the technical analysis report is enclosed in a 1A envelope for inclusion in the case file.

b6
b7C

♦♦

~~SECRET~~ // ~~NOFORN~~

3/24/16
Serial 20

~~SECRET~~

b6
b7c

~~SECRET~~

HRC-8848

~~SECRET//NOFORN~~ [redacted] (S)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE b1 b3 b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 3/24/2016

To: Washington Field

From: Washington Field

CI-13

Contact: IA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

Case ID #: (S) [redacted] CYBER - 2e

(U) Title: (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

(U) Synopsis: (S//NF) To document research and analysis results for
two email addresses and three IP addresses associated with [redacted]
[redacted]

~~Classified By: F36M12K15~~
~~Derived From: FBI NSIC dated 20130301~~
~~Declassify On: 20410223~~

b1
(S) b3
b7E

~~SECRET//NOFORN~~ [redacted] (S)

HRC-8849

b1
b3
b7E

~~SECRET~~//NOFORN [redacted]

(S)

FEDERAL BUREAU OF INVESTIGATION

(S)

b1
b3
b7E

(U)

Details: ~~(S//NF)~~ Investigative activity conducted under captioned investigation revealed [redacted] set up [redacted] in order to facilitate the migration of the Bryan Pagliano (PAGLIANO) server content to Platte River Network's (PRN) infrastructure. A second email address, [redacted] was also identified but found to be his personal account. [redacted] for the two email addresses revealed [redacted] IP addresses were used to log in to both accounts between March and August 2015. Writer queried all [redacted] IP addresses, which are as follows:

b6
b7C
b7E

[redacted]

(S)

b1
b3
b6
b7C
b7E

(S)

(U)

¹ ~~(S//NF)~~ [redacted] an employee of Platte River Networks (PRN) was one of the individuals responsible for migrating the Bryan Pagliano (PAGLIANO) server to PRN in 2013.

b6
b7C

~~SECRET~~//NOFORN [redacted]

(S)

b1
b3
b7E

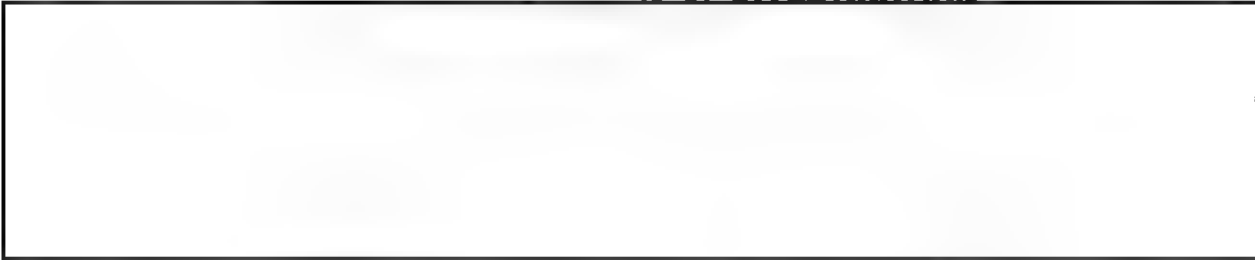
HRC-8850

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

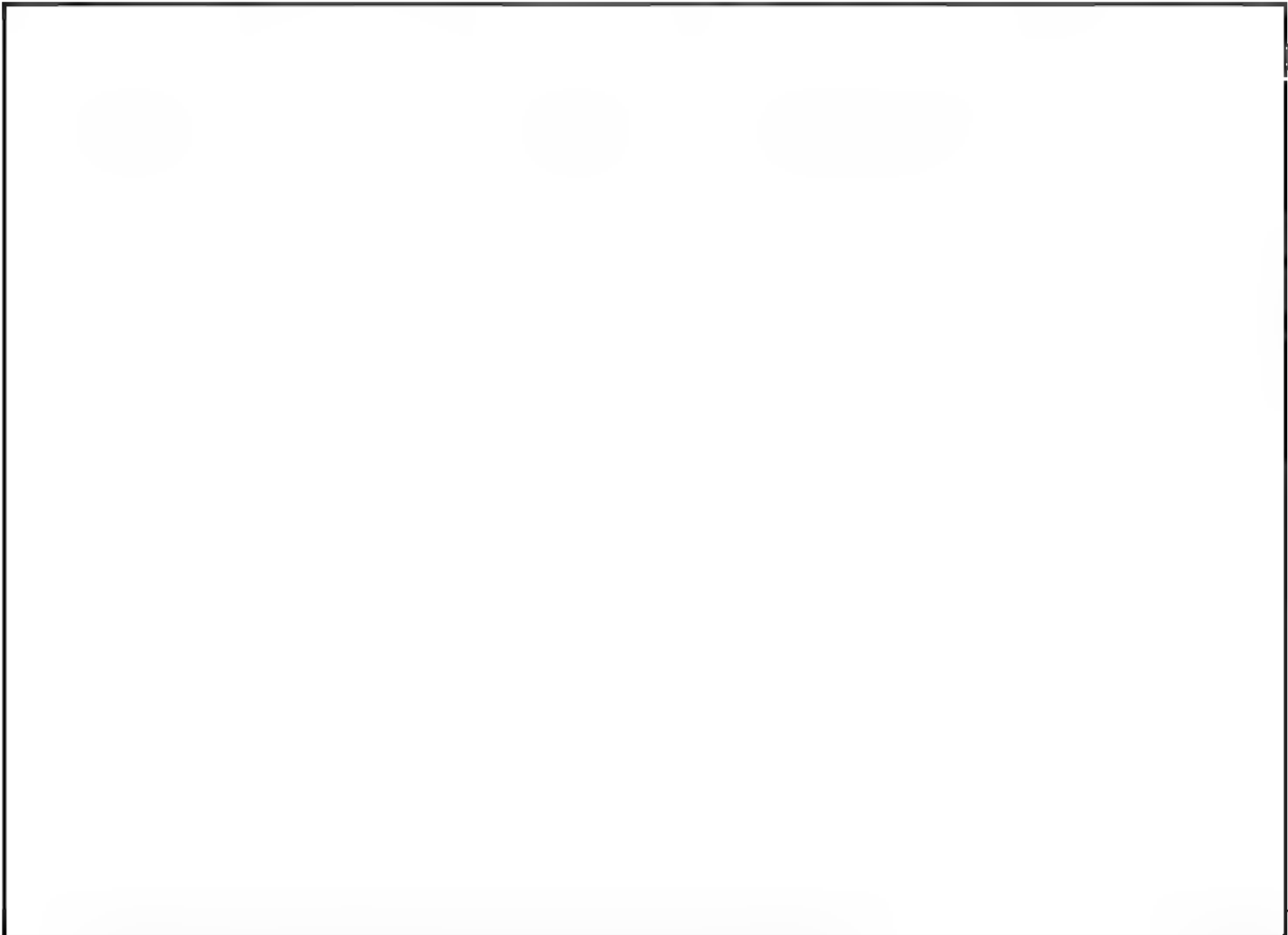


(S)

b1
b3
b7A
b7E

(U//~~FOUO~~) A printout of the [redacted] results for IP address [redacted] is enclosed in a 1A envelope for the case file.

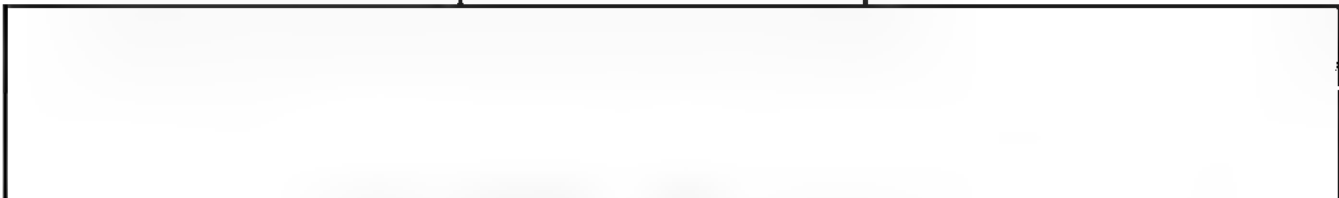
b6
b7C
b7E



(S)

b1
b3
b6
b7C
b7E

(U) Query Results for [redacted]



(S)

b1
b3
b7E

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8851

~~SECRET~~//NOFORN [redacted]

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) [redacted] Email Addresses

(U//~~FOUO~~) A search for [redacted]
and [redacted] in Sentinel, [redacted] and [redacted]
yielded negative results. Information related to the
identification of these accounts and [redacted] the collection of
their use can be found in two in-person interviews with
[redacted] the first conducted on 15 September 2015 (see MIDYEAR
EXAM, 302 Sub-folder, serial 21) and the second on 17 February
2015 (FD-302 not serialized as of the date of this
communication).

b6
b7C
b7E

♦♦

~~SECRET~~//NOFORN [redacted]

(S)

b1
b3
b7E

HRC-8854

3/20/16
Serial 21

~~SECRET~~

b6
b7c

HRC-8855

~~SECRET~~

~~SECRET//NOFORN~~ [redacted] (S)

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b3
b7E

Precedence: ROUTINE

Date: 3/28/2016

To: Washington Field

From: Washington Field

CI-13

Contact: IA [redacted]

Approved By: [redacted]

Drafted By: [redacted]

(U) **Case ID #:** (S) [redacted] -CYBER -21

b3
b6
b7C
b7E

(U) **Title:** (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

(U) **Synopsis:** (S//NF) To document research and analysis results for
email addresses in new confirmed classified not previously
identified.

~~Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410328~~

b1
b3
b7E

~~SECRET//NOFORN~~ [redacted] (S)

b1
b3
b7E

HRC-8856

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

FEDERAL BUREAU OF INVESTIGATION

(S)

b1
b3
b7E

(U) Details: (~~S~~//~~NF~~) On or about 7 March 2015, the MIDYEAR EXAM Investigative Team received [redacted] for messages not part of the original confirmed classified group of emails. Sender and recipient email addresses were extracted from the new messages and compared to a list of email addresses already researched and documented in MIDYEAR EXAM, Cyber sub-folder, serial 8. Writer identified two new email addresses:

b7E

b6
b7C

(U//~~FOUO~~) [redacted]

(S)

b1
b3
b6
b7C
b7E

b7E

(U//~~FOUO~~) [redacted] results are included on a disc in a 1A envelope for the case file.

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8857

~~SECRET//NOFORN~~ [redacted]

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

(U//FOUO) [redacted]

b6
b7C
b7E

(U) [redacted] ~~(S//NF)~~ A search for the email address in [redacted] and [redacted] yielded negative results. Positive returns were identified in Sentinel and [redacted]

(U) Sentinel Results

[Large redacted box]

(S)

b1
b3
b6
b7A
b7C
b7E

(U) [redacted] Results

[Large redacted box]

(S)

b1
b3
b6
b7C
b7E

(U//FOUO) [redacted] results are included on a disc in a 1A envelope for the case file.

b7E

(U//FOUO) Research on Two Additional Email Addresses in Original Group of Confirmed Classified Messages

(U) ~~(S//NF)~~ A review of all unique email addresses found in confirmed classified messages to date revealed two accounts not previously identified by writer:

[Redacted box]

b7E

~~SECRET//NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8858

~~SECRET~~//NOFORN [redacted]

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

(U) Queries for both yielded the following:

(U//~~FOUO~~) [redacted]

b7E

(U//~~FOUO~~) A search for the email address in [redacted] and [redacted] yielded negative results. Positive returns were identified in Sentinel and [redacted]

(U) Sentinel Results

[redacted]

(S)

b1
b3
b7E

(U) [redacted] Results

[redacted]

(S)

b1
b3
b7A
b7E

(U//~~FOUO~~) [redacted] results are included on a disc in a 1A envelope for the case file.

b7E

(U//~~FOUO~~) [redacted]

b7E

(U//~~FOUO~~) A search for the email address in [redacted] and [redacted] yielded negative results. Positive returns were identified in Sentinel and [redacted]

(U) Sentinel Results

[redacted]

(S)

b1
b3
b7A
b7E

~~SECRET~~//NOFORN [redacted]

(S)

HRC-8859

~~SECRET~~ // ~~NOFORN~~ []

(S)

FEDERAL BUREAU OF INVESTIGATION

[Redacted]

(S)

b1
b3
b7A
b7E

(U) [] Results

[Redacted]

(S)

b1
b3
b7E

(U//~~FOUO~~) [] results are included on a disc in a 1A envelope for the case file.

b7E

(U) Summary of Findings

[Redacted]

(S)

b1
b3
b6
b7C
b7E

♦♦

~~SECRET~~ // ~~NOFORN~~ []

(S)

b1
b3
b7E

HRC-8860

4/1/16
Serial 22

~~SECRET~~

b6
b7c

~~SECRET~~

HRC-8861

~~SECRET~~ // ~~ORCON~~ / ~~NOFORN~~ [REDACTED]

(S)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 3/31/2016

To: Washington Field

From: Washington Field
CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) Case ID #: (S) [REDACTED] -CYBER - 22

(U) Title: (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: [REDACTED]

Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410331

~~SECRET~~ // ~~ORCON~~ / ~~NOFORN~~ [REDACTED]

(S)

HRC-8862

b1
b3
b7E

~~SECRET~~/ORCON/NOFORN [redacted] (S)

FEDERAL BUREAU OF INVESTIGATION

b1
(S) b3
b7E

(U) **Details:** ~~(S//NF)~~ As documented in MIDYEAR EXAM, Cyber sub-file, serial 10, Cyber Division's Technical Operations Unit (TOU) analyzed the forensic image of a Lexar Micron 16GB USB device with the purpose of trying to identify malicious content on the device. Several malicious attachments were found in the email archive located on the USB, which TOU subsequently analyzed and categorized into two separate incidents.

b1
(S) b3
b6
b7C
b7E

X

(U) IP Address [redacted]

b1
b3
(S) b7E

~~SECRET~~/ORCON/NOFORN [redacted] (S)

b1
b3
b7E

HRC-8863

~~SECRET~~ // ~~ORCON~~ / ~~NOFORN~~

(S)

FEDERAL BUREAU OF INVESTIGATION

X

(S)

b1
b3
b6
b7A
b7C
b7E

(U) Malicious Attachment's Beacons Information

(S)

b1
b3
b6
b7A
b7C
b7E

(U) Summary of Findings

(S)

b1
b3
b6
b7C
b7E

~~SECRET~~ // ~~ORCON~~ / ~~NOFORN~~

(S)

HRC-8864

~~SECRET~~/ORCON/NOFORN



(S)

FEDERAL BUREAU OF INVESTIGATION



(S)

b1
b3
b7E

(U//~~FOUO~~) A printout  is
enclosed in a 1A envelope for the case file.

♦♦

~~SECRET~~/ORCON/NOFORN



(S)

b1
b3
b7E

HRC-8865

4/11/16
Serial 23

~~SECRET~~

b6
b7c

HRC 8866

~~SECRET~~

~~SECRET~~/NOFORN [redacted] (S)

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 04/04/2016

To: Washington Field

From: Washington Field

CI-13

Contact: [redacted]

b3
b6
b7C
b7E

Approved By: [redacted]

Drafted By: [redacted]

(U) Case ID #: (S/NOFORN) [redacted] CYBER - 23

(U) Title: (S/NOFORN) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//FOUO) Summary of FBI database searches of indicators identified from open source research.

~~Classified By: C21W96B63
Derived From: FBI NSIC dated 20130301
Declassify On: 20410204~~

(U)

References: (S/NOFORN) [redacted] -CYBER, Serial 2; [redacted]
Serial 141; [redacted] -CYBER, Serial 13

b3
b7E

(S)

b1
b3
b7E

~~SECRET~~/NOFORN [redacted] (S)

b1
b3
b7E

~~SECRET~~//~~NOFORN~~ [redacted] (S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION



(S)

b1
b3
b7E

Details:

(U//~~FOUO~~) Searches of open source datasets were used to identify IP addresses and domains directly associated with or related to the Internet domain "clintonemail.com" (see [redacted] Serial 141). These indicators were then searched in FBI databases, and the results of these searches are listed below. In most cases, searches with positive results were documented previously in separate ECs within the case file, so this EC will provide summary results for each indicator, and reference ECs with additional details for indicators with positive hits that were documented previously.

b3
b7E

~~SECRET~~//~~NOFORN~~ [redacted] (S)

b1
b3
b7E

~~SECRET~~ / ~~NOFORN~~ [] (S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

~~(S)~~ / ~~NF~~ []

[] (S)

b1
b3
b7E

(U//~~FOUO~~) DETAIL: A search of [] for clintonemail.com returned positive results. These results are documented in a separate EC: []-CYBER, Serial 2.

~~(S)~~ / ~~NF~~ []

[] (S)

b1
b3
b7E

~~(S)~~ / ~~NF~~ []

[] (S)

b1
b3
b7E

~~(S)~~ / ~~NF~~ []

[] (S)

b1
b3
b7E

(U//~~FOUO~~) DETAIL: A search of [] for presidentclinton.com returned positive results. These results are documented in a separate EC: []-CYBER, Serial 2. A search of Sentinel yielded references to the same activity found in [] which is described in the serial mentioned above. Details of the information found in [] can is documented in a separate EC as well: []-CYBER, Serial 13.

~~(S)~~ / ~~NF~~ []

[] (S)

b1
b3
b7E

~~(S)~~ / ~~NF~~ []

[] (S)

~~SECRET~~ / ~~NOFORN~~ [] (S)

b1
b3
b7E

~~SECRET~~//NOFORN

(S)

FEDERAL BUREAU OF INVESTIGATION



b1
b3
b7E

~~(S)~~//NF



b1
b3
b7E

(S)

~~(S)~~//NF



b1
b3
b7E

(S)

~~(S)~~//NF



(S)

b1
b3
b7E

(U//FOUO) DETAIL: This search produced several positive hits but all from before 06/2013 when [redacted] shows the presidentclinton.com and clintonemail.com domains were resolving here (see [redacted] Serial 141 for full [redacted] details).

~~(S)~~//NF



(S)

b1
b3
b7E

~~SECRET~~//NOFORN

(S)

b1
b3
b7E

~~SECRET~~//NOFORN []

(S)

FEDERAL BUREAU OF INVESTIGATION

b1
b3
b7E

~~SECRET~~//NF []

(S)

b1
b3
b7E

~~SECRET~~//NF []

(S)

b1
b3
b7E

(U//FOUO) DETAIL: A search of [] for [] returned positive results. These results are documented in a separate EC: []-CYBER, Serial 13.

~~SECRET~~//NF []

(S)

b1
b3
b7E

(U//FOUO) DETAIL: A search of [] for [] returned positive results. These results are documented in a separate EC: []-CYBER, Serial 13.

~~SECRET~~//NF []

(S)

b1
b3
b7E

(U//FOUO) Separate ECs were written documenting the specifics of all positive search results documented above (see references). Any recommended investigative follow-up will be documented within the referenced documents.

♦♦

~~SECRET~~//NOFORN []

(S)

b1
b3
b7E

4/11/16
Serial 24

~~SECRET~~

b6
b7c

HRC 8873

~~SECRET~~

~~SECRET~~//NOFORN

FEDERAL BUREAU OF INVESTIGATION

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

Precedence: ROUTINE

Date: 04/07/2016

To: Washington Field

From: Washington Field

CI-13

Contact: SA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) Case ID #: ~~(S)~~ [REDACTED] CYBER -24

(U) Title: ~~(S)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) Documents analysis of failed login attempts and observed firewall activities subsequent to the public disclosure of HILLARY CLINTON's use of a private email server and the personal email address of hdr22@clintonemail.com.

~~Classified By: J91J44T84
Derived From: FBI-NSIC dated 20130301
Declassify On: 20410407~~

Reference: [REDACTED] CYBER-7

Details: (U//~~FOUO~~) This investigation has determined that on 03/02/2015 the NEW YORK TIMES published an article documenting HILLARY CLINTON's use of a private email server and her personal email address of hdr22@clintonemail.com. As to be expected, the public release of that information led to the increase of firewall activity and failed login attempts to the exchange server operating behind that domain.

(U//~~FOUO~~) The above referenced serial documents an analysis performed on suspicious login attempts to an APPLE ICLOUD account associated with email address hdr22@clintonemail.com. That analysis

~~SECRET~~//NOFORN

b3
b6
b7C
b7E

b3
b7E

~~SECRET~~//NOFORN

FEDERAL BUREAU OF INVESTIGATION

revealed that multiple cyber actors had attempted to gain unauthorized access to the ICLOUD account subsequent to the NEW YORK TIMES article. Similarly, a review of firewall and IIS logs for the clintonemail.com exchange server identified that it was targeted in the same manner. Agent Note: The scope of this analysis only includes the review of logs created subsequent to 03/02/2015. Writer did not attempt to review every firewall and IIS logs for this analysis.

~~(U//FOUO)~~ EXCHANGE SERVER - IIS LOGS

(U//~~FOUO~~) The table below depicts the most frequent user accounts which did not successfully authenticated to the exchange server, yet were used for at least two failed login attempts.

(U//FOUO) USER ACCOUNT NAME	# ATTEMPTS

b6
b7C
b7E

~~SECRET~~//NOFORN

~~SECRET~~//~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) As shown on the previous page, the user accounts of

b7E

[REDACTED]
[REDACTED] were most frequently used for failed login attempts. This was also expected, as the targeting of known or suspected user accounts is consistent with that of malicious cyber actors.

(U//~~FOUO~~) The failed login attempts with usernames including the [REDACTED] handle could be attributed to attackers who gleaned the account information from the NEW YORK TIMES article. However, the failed login attempts during this time frame could also be attributed to that of a legitimate user who accidentally entered an invalid password. More indicative of potential cyber attackers, however, are the failed login attempts that occurred with the usernames of [REDACTED] and [REDACTED]

b7E

(S//~~NF~~) In analyzing the failed login attempts to the non-existent [REDACTED] account, writer identified [REDACTED] that originated from IP addresses [REDACTED]

b1
b3
b7E

(S//~~NF~~) In addition, writer identified that IP addresses [REDACTED]

b1
b3
b7E

[REDACTED] were used for login attempts on the non-existent [REDACTED] account; and [REDACTED] and [REDACTED] were used for login attempts on the [REDACTED] account [REDACTED]

(S)

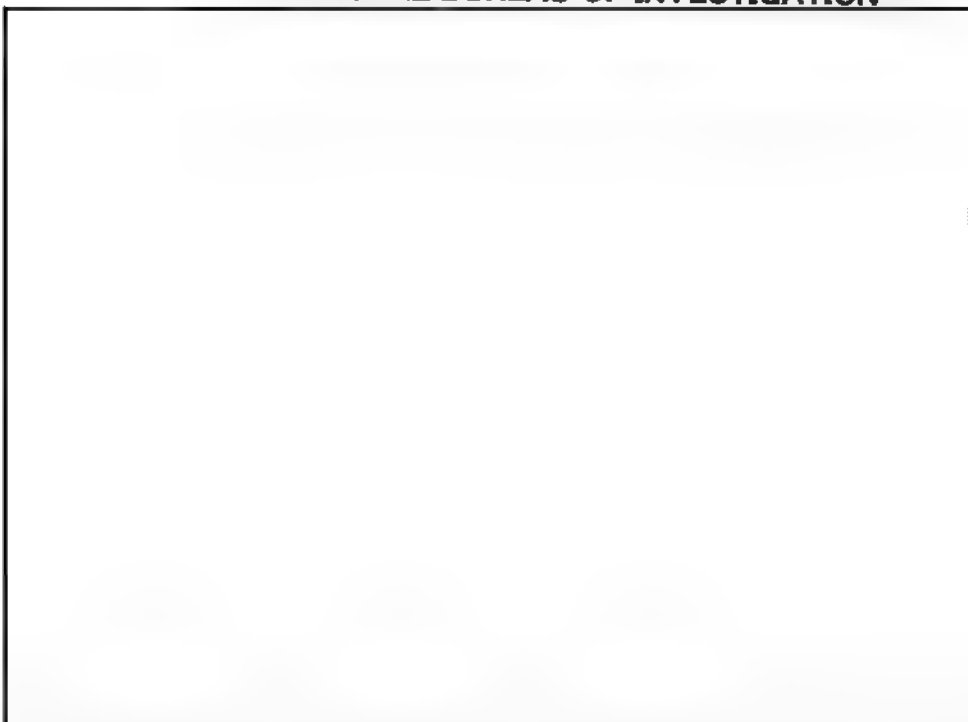
[REDACTED] The chart on the following page summarizes [REDACTED]

[REDACTED] For the purpose of this document, writer did not provide a complete analysis of [REDACTED] as these were only failed attempts.

~~SECRET~~//~~NOFORN~~


~~SECRET~~//~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION






(S)

b1
b3
b7A
b7E

(U//~~FOUO~~) In addition to the repeated failed login attempts from the accounts above, the following user account names were also used for at least one failed login attempt on the exchange server: 

b6
b7C
b7E



 Agent Note: Some of these attempts could have been a result of a mistyped username from a legitimate user; for example,  and 

~~SECRET~~//~~NOFORN~~

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) DOMAIN CONTROLLER FIREWALL LOGS

(U//~~FOUO~~) For this analysis, writer also reviewed the firewall logs obtained from the domain controller associated with the clintonemail.com domain. That review identified that subsequent to 03/02/2015, several unauthorized access attempts were also captured by the firewall. Those attempts are depicted in the following table:



b7E

(U//~~FOUO~~) As shown in the table, the domain controller firewall captured unauthorized login attempts using several fictitious names. Some of those events originated from IP addresses overseas. Writer opines that this is also expected behavior, given the public release of the clintonemail.com domain.

♦♦

~~SECRET//NOFORN~~

4/11/10
Serial 25

~~SECRET~~

b6
b7c

~~SECRET~~

HRC-8879

~~SECRET//NOFORN~~

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 4/8/2016

To: Washington Field

From: Washington Field

CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) Case ID #: (S) [REDACTED] CYBER -25

(U) Title: (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//FOUO) To document queries related to various devices obtained through the course of investigation.

~~Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410408~~

Details: (U//FOUO) IA [REDACTED] Cyber Division, on or about 10 February 2015 received a Microsoft Excel spreadsheet with approximately [REDACTED] identifiers associated with a number of electronic devices identified through the course of captioned investigation. The identifiers were obtained directly off the devices or through subpoena returns. IA [REDACTED] queries on all unique values yielded negative results in [REDACTED]

(U//FOUO) On or about the date of this document, writer received [REDACTED] additional identifiers and subsequently queried the new values. To be thorough, writer also conducted [REDACTED] queries on the [REDACTED] values previously identified.

(S//NF) Writer found results for [REDACTED] of the identifiers: [REDACTED] [REDACTED] are referenced in separate Public Corruption investigations [REDACTED] (S) [REDACTED] No additional research was conducted on [REDACTED] given that [REDACTED] [REDACTED]

~~SECRET//NOFORN~~

HRC-8880

~~SECRET~~//NOFORN

FEDERAL BUREAU OF INVESTIGATION

(U//FOUO) A printout of the results is enclosed in a 1A envelope for the case file.

b7E

♦♦ |

~~SECRET~~//NOFORN

HRC-8881

4/13/16
Serial 26

b6
b7c

HRC-8882

5/13/06
Serial 27

b6
b7C

HRC-8886

FEDERAL BUREAU OF INVESTIGATION

Date: 05/11/2016

Contact: IA

HRC-8887

b7E

~~SECRET~~ // ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION



b3
b7E

(U//~~FOUO~~) Analysis of all [redacted]
[redacted] in general, reveal [redacted]
[redacted]

b3
b7E

² (U//~~FOUO~~) [redacted] provided [redacted] records from [redacted]
[redacted] however, were not supplied to the FBI (NFI).

b3
b7E

~~SECRET~~ // ~~NOFORN~~

HRC-8888

~~SECRET~~//~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U) [redacted]

(U//FOUO) In addition to [redacted] and [redacted] writer also reviewed [redacted] Within the date range, there are some dates for which [redacted] was not found in records subpoenaed from [redacted] As such, writer only reviewed [redacted] in the FBI's possession.

b3
b7E

(U//FOUO) [redacted]

[redacted] For the purpose of analysis supporting captioned investigation, writer reviewed [redacted]

b3
b7E

b3
b7E

(U//FOUO) [redacted]

[redacted] along with [redacted] findings, were compiled for further analysis in Microsoft Excel worksheets, which are enclosed on a disc in a 1A envelope for the case file.

b3
b7E

(U//FOUO) As part of the analysis conducted, writer queried [redacted] against the respective date's [redacted] IIS logs. If [redacted] was found in the corresponding date's IIS logs, writer isolated the activity for further analysis. The majority of the [redacted] were not found in [redacted] searched. Writer surmises that this is due to the fact that [redacted]

b3
b7E

~~SECRET~~//~~NOFORN~~

HRC-8889

~~SECRET~~//~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

[REDACTED]

b3
b7E

(U//~~FOUO~~) ANALYST NOTE: It remains unclear what the

[REDACTED]

b3
b7E

[REDACTED] As such, the FBI supposes that the

[REDACTED]

b3
b7E

[REDACTED]

(U)

X —

—

—

~~SECRET~~//~~NOFORN~~

HRC-8890

~~SECRET~~//NOFORN

FEDERAL BUREAU OF INVESTIGATION

b3
b7E

[REDACTED]
[REDACTED] Overall, writer surmises that [REDACTED]
[REDACTED] was attempting to [REDACTED]
[REDACTED] for unknown reasons.

b3
b7E

[REDACTED]

(U//~~FOUO~~) When news of the existence of the CESC mail server broke public in early March 2015, numerous online media outlets reported details about the server. Around that time and seemingly as a result of some of the articles, [REDACTED]

b3
b6
b7C
b7E

[REDACTED]

(U//~~FOUO~~) Given the publicity related to the server beginning in March 2015, writer assesses that an unidentified

~~SECRET~~//NOFORN

HRC-8891

~~SECRET~~//NOFORN

FEDERAL BUREAU OF INVESTIGATION

individual possibly queried CLINTONEMAIL.COM using [REDACTED]
[REDACTED] to learn more about the server's configuration in August
2015.

b7E

♦♦

~~SECRET~~//NOFORN

HRC-8892

5/10/16
Secret 28

b6
b7C

HRC 8893

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/17/2016

To: Washington Field

From: Washington Field
CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** (S) [REDACTED] -CYBER-18

(U) **Title:** (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//FOUO) To document subpoena returns for [REDACTED]

~~Classified By: F36M12K15
Derived From: FBI-NSIC dated 20130301
Declassify On: 20410517~~

Reference: [REDACTED] -CYBER-24
[REDACTED] -GJ-1A-56
[REDACTED] -GJ-1A-57
[REDACTED] -GJ-1A-58
[REDACTED] -GJ-1A-59

Details: (U//FOUO) The FBI's Operational Technology Division (OTD) successfully extracted a limited number of domain controller logs captured by the CESC FORTIGATE80C firewall. OTD subsequently provided logs for March 3-5, 2015 to the MIDYEAR EXAM Investigative Team, which SA [REDACTED] analyzed on or about March 29, 2016. A log for March 22, 2013 was also extracted by OTD and analyzed by writer.

(U) DOMAIN CONTROLLER LOGS FOR MARCH 3-5, 2015

(U//FOUO) Per referenced serial, SA [REDACTED] identified approximately [REDACTED] IP addresses that were unsuccessful in attempting to log in to the domain controller subsequent to March 2, 2015, the day THE NEW YORK TIMES published an article documenting HILLARY RODHAM CLINTON's use of a private email

~~SECRET//NOFORN~~

HRC-8894

~~SECRET~~ / ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

server and her use of HDR22@CLINTONEMAIL.COM. [Reference:
MIDYEAR EXAM, [REDACTED] CYBER-24]

b3
b6
b7C
b7E



(U//~~FOUO~~) A determination was made by the MIDYEAR EXAM
Investigative Team to not interview [REDACTED]
given that the login attempts were unsuccessful.

b6
b7C
b7E

~~SECRET~~ / ~~NOFORN~~

HRC-8895

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U) DOMAIN CONTROLLER LOG FOR JUNE 22, 2013

(U//~~FOUO~~) OTD was also able to extract one file from a log directory on Firewall A, found specifically at [REDACTED]. OTD identified the file because, when looking at the domain controller server natively, there was reference to the foregoing path as a log directory when authentication is enabled.

b7E

(U//~~FOUO~~) The log contained login information for [REDACTED] which writer analyzed. [REDACTED] IP addresses were used to log in to the account [REDACTED]

b3
b6
b7C
b7E

♦♦

~~SECRET//NOFORN~~

HRC-8896

5/19/16
Serial 29

b6
b7c

HRC 8897

~~SECRET~~ // NOFORN

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 05/17/2016

To: Washington Field

From: Washington Field
CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** ~~(S)~~ [REDACTED]-CYBER-29

(U) **Title:** ~~(S)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To document details related to the classification of foreign policy and intelligence memos authored by SIDNEY BLUMENTHAL, and the finding of one of the memos in the GUCCIFER ARCHIVE.

~~Classified By: F36M12K15~~
~~Derived From: FBI NSIC dated 20130301~~
~~Declassify On: 20410517~~

Reference: (U) ~~(S)~~ [REDACTED]-CYBER-6

Details: (U) SIDNEY BLUMENTHAL (BLUMENTHAL) is a former political aide to President WILLIAM J. CLINTON and served as an advisor to HILLARY RODHAM CLINTON (CLINTON) during her tenure as Secretary of State, often providing her memos on various foreign policy and intelligence matters.

(U) BLUMENTHAL Memo Classifications

(U//~~FOUO~~) On or about May 13, 2016, ITSPEC/FE [REDACTED] and writer extracted [REDACTED] for all available foreign policy and intelligence memos authored by BLUMENTHAL and sent to CLINTON. A total of [REDACTED] unique memos were identified [REDACTED]. Separately, [REDACTED] and writer queried [REDACTED] for all Microsoft Word documents tagged with the labels "SID" and "B1," the latter of which signifies the document was deemed CONFIDENTIAL following classification review. The list of B1 memos, totaling [REDACTED] were extracted in a separate Microsoft Excel spreadsheet.

~~SECRET~~ // NOFORN

HRC-8898

b3
b6
b7C
b7E

b3
b7E

b6
b7C
b7E

~~SECRET~~ // NOFORN

FEDERAL BUREAU OF INVESTIGATION

(U//FOUO) In an effort to ensure the [] memos were also captured in the list of [] writer compared both data sets. For unknown reasons but likely due to [] used to pull all memos, only [] of the [] memos tagged B1 were found in the larger set. The [] not found were []

b7E

(U//FOUO) In addition to the [] memos tagged B1, writer is also aware of another BLUMENTHAL memo deemed SECRET after classification review []. Given its classification, writer did not expect the memo to be listed in the B1 list. [] were compiled for the [] classified memos ([] CONFIDENTIAL and [] SECRET).

b7E

(U//FOUO) Writer additionally compared the list of known classified memos to an open source article published by The Daily Caller on March 7, 2016, which claimed BLUMENTHAL sent CLINTON 23 classified memos. The list of 23, however, contained four emails whose text was redacted in part or full. One of the emails contained an attached memo, but there is no indication the totality (or parts) of the document was released through the Freedom of Information Act (FOIA) process. The remaining 18 items []

b7E

(U//FOUO) In sum, BLUMENTHAL authored [] memos deemed CONFIDENTIAL and [] deemed SECRET. All memos were transmitted utilizing his AOL account, []

b6
b7C
b7E

(U) CLINTON Server Breach Allegations []

(U//FOUO) In early May 2016, MARCEL LEHEL LAZAR (LAZAR) publicly alleged he breached the CLINTON server in early 2013, shortly after compromising BLUMENTHAL'S AOL account. LAZAR, also known as 'GUCCIFER,' claimed he used the compromise of BLUMENTHAL'S account as a stepping stone to the CLINTON server. Details about the allegations and analysis of the server logs will be documented in a separate document.

(U//FOUO) Subsequent to LAZAR'S claims, writer contacted []

b6
b7C
b7E

~~SECRET~~ // NOFORN

HRC-8899

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) On May 16, 2016 SA [redacted] confirmed that [redacted] The memo [redacted] and FOIA Case No. F-2014-20439, Doc. No. C05792899) is deemed CONFIDENTIAL and was entirely redacted when released through the FOIA process. GUCCIFER almost certainly obtained a copy of the now-classified memo when he hacked BLUMENTHAL's AOL account.

b6
b7C
b7E

(U//~~FOUO~~) [redacted]
[redacted]

(U//~~FOUO~~) Correction to [redacted]-CYBER, Serial 6

b3
b7E

(U//~~FOUO~~) Referenced serial, which detailed LAZAR's compromise of BLUMENTHAL's AOL account, erroneously made references to CLINTON exchanging emails with BLUMENTHAL using her HROD17@CLINTONEMAIL.COM account. Writer also speculated that the FBI could not discount the possibility of LAZAR having searched for correspondence between BLUMENTHAL and her 'HROD17' account. After consulting with MIDYEAR EXAM Investigative Team colleagues, writer determined HROD17@CLINTONEMAIL.COM was not created until after the BLUMENTHAL's account breach. Therefore, there was no correspondence between BLUMENTHAL and 'HROD17'; BLUMENTHAL's exchanges were only with CLINTON's 'HDR22' account.

(U) According to a fact sheet released by HILLARYCLINTON.COM, CLINTON

Used only one email account during her tenure at State [...] In March 2013, a month after she left the Department, Gawker published the email address she used while Secretary, and so she had to change the address on her account. At the time the printed copies were provided to the Department in 2014, because it was the same account, the new email address established after she left office appeared on the printed copies as the sender, and not the address she used as Secretary. In fact, this address on the account did not exist until March 2013.

(U//~~FOUO~~) Writer hereby corrects any reference to HROD17@CLINTONEMAIL.COM made in referenced serial, as the only CLINTON account that corresponded with BLUMENTHAL was HDR22@CLINTONEMAIL.COM.

(U//~~FOUO~~) Enclosed for the case file in a 1A envelope are two discs: one contains memos' metadata extracted from [redacted] and the other is writer's compilation and check/sum of known classified memos. [redacted]
[redacted]

b7E

~~SECRET//NOFORN~~

HRC-8900

~~SECRET~~ / ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

[Redacted]

b7E

The fact sheet referenced above is also enclosed.

♦♦

~~SECRET~~ / ~~NOFORN~~

HRC-8901

4/9/16
Serial 30

b6
b7C

HRC 8902

~~SECRET~~/NOFORN

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/05/2016

To: Washington Field

From: Washington Field

CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** ~~(S)~~ [REDACTED] -CYBER -30

(U) **Title:** ~~(S)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To memorialize subpoena returns for [REDACTED]

[REDACTED]

~~Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410605~~

Reference: (U) ~~(S)~~ [REDACTED] -CYBER-27
(U) ~~(S)~~ [REDACTED] -GJ-61

Details: (U//~~FOUO~~) In support of captioned investigation,
writer reviewed subpoena returns obtained from [REDACTED]
[REDACTED] Email furnished by [REDACTED]

[REDACTED]

(U//~~FOUO~~) Analysis of the [REDACTED] identified [REDACTED]

[REDACTED]

[REDACTED] Open source research indicated the
[REDACTED] allows a remote attacker
to execute arbitrary code and cause a denial of service (DoS)
attack.

(U//~~FOUO~~) Subpoenas were issued for [REDACTED]

[REDACTED]

~~SECRET~~/NOFORN

HRC-8903

b3
b6
b7C
b7E

b3
b7E

b3
b7E

b3
b7E

b3
b7E

b3
b7E

~~SECRET~~ // ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U)



b3
b7E

(U//~~FOUO~~) A determination was made by the MIDYEAR EXAM
Investigative Team to not interview [redacted]

b3
b7E



[redacted] (see [redacted] CYBER, serial
27).

♦♦

~~SECRET~~ // ~~NOFORN~~

HRC-8904

4/5/14
Serial 31

b6
b7c

HRC-8905

u/s/16
Serial 32

b6
b7C

HRC 8910

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/02/2016

To: Washington Field

From: Washington Field
CI-13

Contact: SA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** ~~(S)~~ [REDACTED] CYBER - 32

(U) **Title:** ~~(S)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) Documents investigative actions taken in response to allegations that Romanian hacker, MARCEL LEHEL LAZAR, aka "GUCCIFER", hacked HILLARY CLINTON's (CLINTON) email server in March of 2013.

~~Classified By: J91J44T84
Derived From: FBI NSIC dated 20130301
Declassify On: 20410602~~

Details: (U//~~FOUO~~) On 05/04/2016 and 05/07/2016, FOX NEWS released two news articles reporting that Romanian hacker MARCEL LEHEL LAZAR (LAZAR), aka "GUCCIFER", had allegedly claimed to have hacked the clintonemail.com server in March of 2013. Those two news articles were derived from a series of interviews that FOX NEWS conducted with LAZAR from his jail cell in Virginia.

(U) FOX NEWS ARTICLES

(U//~~FOUO~~) According to those articles, LAZAR reportedly hacked the clintonemail.com server "like twice", using an initial compromise vector of SIDNEY BLUMENTHAL's (BLUMENTHAL) AOL account as a stepping stone to the clintonemail.com server. LAZAR stated that from that compromise, he obtained an IP address for the clintonemail.com server from the emails contained in BLUMENTHAL's

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

account. The articles further relayed that LAZAR subsequently utilized readily available computer network tools such as NETSCAN, NETMAP, WIRESHARK, and ANGRYIP, to scan the server and see if it was alive. According to the interviews, LAZAR utilized proxy servers in Russia for his hacking activities, as he believed they afforded him the best anonymity online. FOX NEWS reported no additional details about how LAZAR allegedly hacked into the clintonemail.com server. However, he reportedly stated that it "was easy" and that it followed his normal "four step process", which was to: 1) identify the target, 2) do extensive web research on the target, 3) access the target's account to harvest data, and 4) send victim data to the media.

(U//~~FOUO~~) Printouts of the original FOX NEWS articles are enclosed for the file in a 1A envelope.

(U//~~FOUO~~) FBI INTERVIEW WITH LAZAR ON 05/26/2016

(U//~~FOUO~~) On 05/26/2016, LAZAR was interviewed by the FBI at the UNITED STATES ATTORNEY'S OFFICE (USAO) in Alexandria, Virginia. During that interview, LAZAR denied hacking the CLINTON email server and stated that he had lied to FOX NEWS about that particular issue. LAZAR stated that he did in fact attempt to identify the originating IP address from an email header contained in BLUMENTHAL's account. However, LAZAR stated that he was only able to identify the IP address of 127.0.0.1 for the clintonemail.com domain, which he identified as an internal IP address. LAZAR stated that he assumed the 127.0.0.1 address was likely assigned to a mail server at the AOL service provider and concluded his hacking attempts against the CLINTON server at that time. According to LAZAR's statements during the interview, that encompassed the extent of his hacking activities against the CLINTON server.

(U//~~FOUO~~) LAZAR provided that his compromise of BLUMENTHAL's account occurred on the date of 03/14/2013 and lasted for the duration of approximately six to seven hours. LAZAR recalled that his access was terminated in BLUMENTHAL's account at approximately 08:00 Chicago Time.

(U//~~FOUO~~) During his interview with the FBI, LAZAR described his familiarity with other hacking tools such as METASPLOIT, CAIN AND ABLE, ANGRYIP, and SUBSEVEN. All of these tools are readily available and can be used by hackers in furtherance of gaining

~~SECRET//NOFORN~~

~~SECRET~~//NOFORN

FEDERAL BUREAU OF INVESTIGATION

unauthorized access to systems. LAZAR described the basic functionality of these tools but did not answer specific follow-up questions about their corresponding capabilities and functionalities. Additionally, LAZAR referred to himself as being a script kiddie and an amateur hacker rather than a professional one.

(U//~~FOUO~~) LAZAR provided that he utilized the MOZILLA FIREFOX browser on a Windows-based operating system for conducting his various hacking activities. Furthermore, he attempted to directly log in to systems by typing IP addresses into his browser.

(U//~~FOUO~~) Further details about information provided by LAZAR during his interview with the FBI can be found in the corresponding FD-302 in this case file.

(U//~~FOUO~~) FORENSIC REVIEW OF THE CLINTON SERVER

(U//~~FOUO~~) Given these allegations, writer performed additional follow-up analysis in an effort to further determine whether or not LAZAR was successful in hacking the CLINTON server. FBI investigation has determined that LAZAR's activities with the BLUMENTHAL AOL account occurred on the date of 03/14/2013. Therefore, analytical follow-up in this investigation primarily focused on the review of digital forensics around that time period.

(U//~~FOUO~~) On or about 05/13/2016, writer spoke with the case Agents for [REDACTED] and obtained a list of approximately [REDACTED] IP addresses, which were identified as being used by LAZAR for his hacking activities. Utilizing [REDACTED] writer conducted a search for any reference of those IP addresses in log files that were obtained from the CLINTON server. No references of those IP addresses were found in any of the Microsoft Internet Information Services (IIS) logs on the server.

b3
b7E

(U//~~FOUO~~) Additionally, with the assistance of Computer Scientist (CS) [REDACTED] was created containing [REDACTED] and other files from the CLINTON server. Again using [REDACTED] writer queried the master [REDACTED] file for any references of the GUCCIFER IP addresses and no results were returned.

b7E

~~SECRET~~//NOFORN

~~SECRET~~ / ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) On or about 05/12/2016, writer pulled the unique IP addresses from the 03/2013 IIS logs that were obtained from the CLINTON server. Given that LAZAR reportedly utilized Russian proxies for his hacking activities, writer then attempted to identify any [REDACTED] in the 03/2013 logs. Of interest to this investigation is that [REDACTED]

b7E

[REDACTED]
[REDACTED] A review of the log entry for that IP revealed that it [REDACTED]

(U//~~FOUO~~) An additional log entry was identified on 03/15/2013 at 08:15:54, from an IP address listed as "ee://aol/http". Open source information indicates that this log entry represents an AOL toolbar installed on a browser. An additional review of the [REDACTED] listed for both entries in the IIS logs identified that they both contained [REDACTED]

b7E

[REDACTED] Given that, writer reviewed the 03/2013 IIS logs for additional references of the same [REDACTED] and found several other references of the same. They are listed below along with their corresponding IP addresses and the dates and times that they were referenced in the logs:

b7E

[REDACTED]

(U//~~FOUO~~) The above listed [REDACTED] denotes the [REDACTED] information that is passed along to the server with the request. However, it does not necessarily uniquely identify [REDACTED] Given that, IP addresses [REDACTED] [REDACTED] could be of relevance in this

b7E

~~SECRET~~ / ~~NOFORN~~

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

investigation as they: 1) represent attempts to access an Administrator web page on the server; 2) highlight the attempts were made from IP addresses located in [REDACTED] 3) show that the attempts were made from a Windows operating system with a MOZILLA FIREFOX browser; and 4) that all occurred subsequent to the BLUMENTHAL account compromise. The attempt [REDACTED] is specifically of interest because it occurred around the same time frame in which LAZAR had access to the BLUMENTHAL account.

b7E

(U//~~FOUO~~) Given the findings in this analysis, writer assesses it is possible that LAZAR's statements during the debrief with the FBI on 05/26/2016 may not have been entirely accurate, and that he may have actually identified the X-originating IP address for the CLINTON server during the compromise of BLUMENTHAL's account. Additionally, it is possible that LAZAR may have attempted to access the CLINTON server on at least one occasion-- [REDACTED]

[REDACTED] However, no additional forensic evidence has been identified in this investigation to directly tie LAZAR to the failed attempt [REDACTED]

b7E

(U) [REDACTED]

(U//~~FOUO~~) In support of this analysis, writer also utilized [REDACTED] to query specific search terms through the [REDACTED] file in an effort to identify whether or not certain programs were executed on the system.

b7E

(U//~~FOUO~~) Of interest for this analysis is that writer identified [REDACTED] in the log files for the CLINTON server. The majority of dates listed for the entries occurred in [REDACTED]

b7E

[REDACTED] A review of the logs identified that someone logged in to the Administrator account, downloaded the [REDACTED] program, and ran it. Additionally, writer identified that certain logs did not encompass dates prior to [REDACTED] therefore, a determination could not be made about the same activity in [REDACTED] At this time, it is unknown who downloaded and ran the [REDACTED] program from the Administrator account in 06/2013.

♦♦

~~SECRET//NOFORN~~

4/22/16
Serial 33

~~SECRET~~

b6
b7c

HRC-8916

~~SECRET~~

~~SECRET~~ / ~~NOFORN~~ []

(S)

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/17/2016

To: Washington Field

From: Washington Field
CI-13

Contact: IA []

Approved By: []

Drafted By: []

Case ID #: (S) [] - CYBER - 33

Title: (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//FOUO) To document files found on the desktop of
BRYAN PAGLIANO.

~~Classified By: F36M12K15~~
~~Derived From: FBI NSIC dated 20130301~~
~~Declassify On: 20410617~~

b1
b3
b7E

~~SECRET~~ / ~~NOFORN~~ []

(S)

b1
b3
b7E

HRC-8917

~~SECRET~~ // NOFORN [redacted]

(S)

b1
b3
b7E

FEDERAL BUREAU OF INVESTIGATION

(S)

b1
b3
b7E

Details: (U//FOUO) In support of captioned investigation, various files saved on the desktop of BRYAN PAGLIANO (PAGLIANO) were analyzed. Of interest were three .txt files titled, [redacted]

[redacted] extracted from the three files were queried in FBI databases in an effort to identify any association with previously established malicious activity. The three files can be found in [redacted]

b7E

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

b7E

b7E

[redacted]
[redacted] It remains unknown why PAGLIANO saved these [redacted] in particular when the server is known to repeatedly have experienced brute force attacks.

(U//FOUO) PAGLIANO also saved [redacted]

[redacted]
[redacted] Based on forensic analysis, the PAGLIANO server [redacted]

b1
b3
b7E

~~SECRET~~ // NOFORN [redacted]

(S)

HRC-8918

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

FEDERAL BUREAU OF INVESTIGATION

(S)

b1
b3
b7E

(U//~~FOUO~~) In sum, [redacted]

none of the [redacted] queried in FBI databases were associated with clear cyber intrusion activity.

b7E

(U//~~FOUO~~) It remains unknown why PAGLIANO saved

[redacted] or if he followed up on the data. It also remains unknown if all [redacted] listed in the .txt file were observed on the same day or if PAGLIANO kept a running list of [redacted]

b7E

(U//~~FOUO~~) Printouts of the three .txt documents are enclosed in a 1A envelope for the case file.

♦♦

~~SECRET~~ // ~~NOFORN~~ [redacted]

(S)

b1
b3
b7E

HRC-8920

6/27/16
Serial 35

~~SECRET~~

b6
b7c

HRC 8926

~~SECRET~~

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 06/23/2016

To: Washington Field

From: Washington Field
CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** (S) [REDACTED] -CYBER -35

(U) **Title:** (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//FOUO) Summary of [REDACTED]
[REDACTED]

~~Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410623~~

Reference:

(U) (S) [REDACTED] -CYBER-6
(S) -CYBER-29
(S) -CYBER-31
(S) -CYBER-32

Details: (U//FOUO) FBI Washington Field Office (WFO) provided
[REDACTED]

(U) [REDACTED]

(U//FOUO) In support of captioned investigation,
[REDACTED]

~~SECRET//NOFORN~~

HRC-8927

b3
b6
b7C
b7E

b7E

b3
b7E

b7E

b7E

7/1/16
Sect 36

b6
b7c

HRC 8932 -

7/6/16
Serial 37

b6
b7C

HRC-8939

(Rev. 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION (U)

Precedence: ROUTINE

Date: 07/05/2016

To: Washington Field

From: Washington Field
CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) Case ID #: (S) [REDACTED] CYBER - 37

(U) Title: (S) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//FOUO) To summarize suspicious login activity to [REDACTED] on January 5, 2013.

Classified By: F36M12K15
Derived From: FBI NSIC dated 20130301
Declassify On: 20410705

Reference: (U) (S) [REDACTED] 302, serial 88

Details: (U//FOUO) Per referenced serial, [REDACTED] the user of [REDACTED] was interviewed telephonically by the Federal Bureau of Investigation on June 29, 2016 regarding her knowledge and use of The Onion Router (Tor), a tool that enables anonymous communication on the Internet. [REDACTED] offered she was not familiar with Tor and has never used the tool. Tor, however, was used to successfully log in to [REDACTED] e-mail account on January 5, 2013. A summary of the event is detailed below.

(U//FOUO) On January 5, 2013 [REDACTED] e-mail account, which was hosted on HILLARY CLINTON's personal e-mail server, was successfully accessed from a Tor node [REDACTED]. Based on available log information, the account [REDACTED]. Over the course of [REDACTED] continuous inbox browsing was conducted. While [REDACTED] cannot be determined, analysis of the [REDACTED] [REDACTED] noted that [REDACTED]

~~SECRET//NOFORN~~

HRC-8940

~~SECRET~~ / ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

[REDACTED]

b7E

(U//~~FOUO~~) Given the nature of Tor, the client IP address changed approximately every 8-10 minutes. Over the course of session, three different Tor nodes were logged:

[REDACTED]

b7E

(U//~~FOUO~~) Based on [REDACTED] statements and log information, the FBI assesses [REDACTED] was accessed without authorization on January 5, 2013. It remains unknown how [REDACTED] credentials were compromised, and if any information was exfiltrated from her inbox.

b6
b7C

(U//~~FOUO~~) A disc containing a copy of the IIS logs related to [REDACTED] account for January 5, 2013 is enclosed in a 1A envelope for the case file.

b6
b7C
b7E

♦♦

~~SECRET~~ / ~~NOFORN~~

HRC-8941

7/18/14
Serial 38

b6
b7c

HRC 8942

~~SECRET~~ // ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE

Date: 07/15/2016

To: Washington Field

From: Washington Field
CI-13

Contact: IA [REDACTED]

Approved By: [REDACTED]

Drafted By: [REDACTED]

(U) Case ID #: ~~(S)~~ [REDACTED] - CYBER - 38

(U) Title: ~~(S)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To document analysis of HILLARY RODHAM CLINTON's logins to the BRYAN PAGLIANO Server.

~~Classified By: F36M12K15~~
~~Derived From: FBI NSIC dated 20130301~~
~~Declassify On: 20411231~~

Reference: (U) ~~(S)~~ [REDACTED] - 302, serial 87
~~(S)~~ [REDACTED] - 302, serial 90

Details: (U//~~FOUO~~) On or about June 17, 2016, Operational Technology Division (OTD) provided HILLARY RODHAM CLINTON's (CLINTON) logins to the BRYAN PAGLIANO (PAGLIANO) Server, which was in service from approximately late March 2009 to late June 2013. The data provided by OTD was requested in an effort to identify: when CLINTON may have begun using the PAGLIANO Server for e-mail purposes; possible suspicious login activity while her account was hosted on the PAGLIANO Server; and determine whether logins were conducted from high-threat countries CLINTON traveled to during her tenure as U.S. Secretary of State.

(U//~~FOUO~~) Analysis of e-mail records obtained by the FBI revealed CLINTON began using the e-mail address HDR22@CLINTONEMAIL.COM¹ on or about January 23, 2009, having previously used HR15@ATT.BLACKBERRY.NET. CLINTON's new e-mail address presumably was hosted on the APPLE Server once the

¹ (U//~~FOUO~~) [REDACTED] according to subpoena returns.

~~SECRET~~ // ~~NOFORN~~

HRC-8943

b3
b6
b7C
b7E

b3
b7E

b3
b7E

~~SECRET~~//~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

switch occurred. This assessment is supported by the fact that the PAGLIANO Server was not operational for e-mail until March 19, 2009.

(U//~~FOUO~~) Of note, the FBI was unable to verify if, and for how long, HDR22@CLINTONEMAIL.COM was hosted on the APPLE Server, as the device was not turned over to the FBI for forensic examination. Additionally, investigation to date has not been able to identify the exact date of when HDR22@CLINTONEMAIL.COM was first hosted on the PAGLIANO Server. However, based on e-mail analysis of HUMA ABEDIN's (ABEDIN) U.S. Department of State (STATE) OpenNet account, the first reflection of HDR22@CLINTONEMAIL.COM is on an e-mail dated January 23, 2009 [REDACTED].

b7E

(U//~~FOUO~~) Logins for CLINTON were available from April 18, 2009 to June 30, 2013. There were approximately [REDACTED] events captured in the PAGLIANO Server's Internet Information Services (IIS) logs, with activity stemming from [REDACTED] unique IP addresses. Writer geo-located all IP addresses and found that [REDACTED] resolved to the United States and [REDACTED] to foreign nations.

b7E

(U//~~FOUO~~) Logins from US-Based IP Addresses

(U//~~FOUO~~) Of the [REDACTED] US-based IP addresses, [REDACTED] resolved to public Internet Service Providers (ISPs). [REDACTED] of the remaining [REDACTED] IP addresses resolved to STATE [REDACTED] and [REDACTED] and the other two to the U.S. Air Force [REDACTED]. Logins from the [REDACTED] U.S. Government IP addresses were scrutinized given that CLINTON was not known to have had a computer terminal while at STATE, and repeated logins in 2011 and 2012 from IP addresses resolving to a [REDACTED] seemed unusual.

b7E

(U//~~FOUO~~) Logins Conducted from STATE IP Addresses

(U//~~FOUO~~) Logins from the [REDACTED] STATE IP addresses were conducted on March 12, 2010 [REDACTED]. Based on statements provided to the FBI, which noted a limited number of individuals had authorized access to CLINTON's e-mail account, logins from STATE IP addresses likely were carried out by CLINTON's aides. These individuals had authorized access for a variety of reasons, one of which was to facilitate the retrieval of old messages, as CLINTON's BLACKBERRY devices only held 30 days' worth of e-mail traffic. [Reference: [REDACTED] 302, serials 87 and 90]

b3

b7E

(U//~~FOUO~~) Logins Conducted from USAF IP Addresses

(U//~~FOUO~~) Analysis of logins conducted from [REDACTED] found that CLINTON's account was

b7E

~~SECRET~~//~~NOFORN~~

HRC-8944

~~SECRET//NOFORN~~**FEDERAL BUREAU OF INVESTIGATION**

accessed on numerous occasions in 2011 and 2012 from the [redacted] aforementioned IP addresses. The majority of the events captured denoted [redacted]

b7E

[redacted] It remains unknown why two USAF IP addresses are reflected in the IIS logs; however, a possible explanation is that CLINTON's iPad devices were connected to a USAF network, perhaps the C-32 airplane² she traveled on when on official business. Writer assesses this is a likely explanation, as the dates of activity reflected on the IIS logs correlate with CLINTON's official overseas travel schedule, as published by STATE.

(U//~~FOUO~~) Logins from Foreign IP Addresses

(U//~~FOUO~~) Writer resolved the [redacted] foreign IP addresses, which resulted in the following:

b7E

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

IP Address	Country	Date of Login
[redacted]		

b7E

(U//~~FOUO~~) The date(s) of login activity from each of the above-listed countries was compared to CLINTON's official overseas travel schedule. Writer found that in most cases CLINTON was on official travel to the country from where the login occurred, or in the same geographical region she was on travel to, possibly suggesting a layover or short stop given the proximity in travel dates.

² (U) The C-32 is a military version of the Boeing 757-200 commercial intercontinental airliner. These airplanes are currently used for high-priority personnel transport, to include the U.S. Secretary of State.

~~SECRET//NOFORN~~

HRC-8945

~~SECRET~~//~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) Writer found that logins from [REDACTED] [REDACTED] however, were suspicious, as CLINTON was not on travel to either country or in another close-by nation-state around the date login activity was captured in the IIS logs. In the case of login activity from [REDACTED] on [REDACTED] CLINTON's official travel schedule noted she was in Lebanon on April 26, 2009 and did not travel again on official business until May 31, 2009, when she visited El Salvador. It is unknown if CLINTON [REDACTED] for approximately [REDACTED] after her official travel to Lebanon, though it is a plausible explanation for the [REDACTED] login activity from [REDACTED]

b7E

(U//~~FOUO~~) Other suspicious activity occurred on [REDACTED] from an IP address that resolved to [REDACTED]. According to CLINTON's official overseas travel schedule, she was in Singapore on that date and traveled to the People's Republic of China on November 16, 2009. As such, a login from [REDACTED] seemed unusual.

b7E

(U//~~FOUO~~) Given that CLINTON's tenure as U.S. Secretary of State ended on February 1, 2013, writer was unable to ascertain if there was any correlation between her travel and logins from [REDACTED] in [REDACTED] as the activity occurred almost [REDACTED] after she had left office³.

b7E

(U//~~FOUO~~) Logins Likely Conducted by CLINTON's Aides During and After Her Tenure as U.S. Secretary of State

(U//~~FOUO~~) As mentioned above, select staff members had authorized access to CLINTON's e-mail account during her tenure as U.S. Secretary of State. A closer look at login activity conducted from US-based and overseas locations revealed aides probably were responsible for logins to CLINTON's e-mail account between 2009 and 2013, the duration of CLINTON's tenure.

(U//~~FOUO~~) Logins from US-Based IP Addresses

(U//~~FOUO~~) [REDACTED] analysis of US-based activity revealed repeated logins to CLINTON's account between 2009 and 2013 likely was done by her staff members, judging by [REDACTED]. The activity in question was conducted from IP addresses that resolved to [REDACTED]

b7E

³ (U) CLINTON served as U.S. Secretary of State from January 21, 2009 to February 1, 2013.

~~SECRET~~//~~NOFORN~~

HRC-8946

~~SECRET~~ // ~~NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) While writer was unable to establish with a definite degree of certainty that a significant number of logins were conducted by CLINTON aides, statements provided to the FBI by at least two witnesses make it likely the activity was carried out by CLINTON staff members. As an example, MONICA HANLEY (HANLEY) is known to have created an archive of CLINTON's inbox following the compromise of SIDNEY BLUMENTHAL's personal e-mail in March 2013. HANLEY offered to the FBI that she used an APPLE Macintosh computer shortly thereafter to access CLINTON's e-mail and archive messages. Activity that was reflected in the IIS logs. [Reference: [REDACTED]-302, serials 87]

b3
b7E

(U//~~FOUO~~) Logins from Foreign IP Addresses

(U//~~FOUO~~) Login activity revealed that aides probably were responsible for logins from [REDACTED]. This assessment is based on closer inspection of [REDACTED] associated with the activity, which indicated that [REDACTED] were used to log in to CLINTON's account. Based on statements provided to the FBI, CLINTON is only known to have used BLACKBERRY and APPLE iPad devices to access her account, rendering it likely that logins from [REDACTED] were carried out by CLINTON staff members.

b7E

(U//~~FOUO~~) Logins using [REDACTED] machines were conducted from IP addresses that resolved to the [REDACTED]. Given the above, it is likely that these logins were carried out by CLINTON's aides, as CLINTON did not use [REDACTED] she only utilized iPad devices, which run on APPLE iOS software. Furthermore, this could explain the anomalous logins from [REDACTED] detailed earlier in this document.

b7E

(U//~~FOUO~~) There is insufficient data to determine if connections to the CLINTON server from overseas were conducted from public or secure networks. As a consideration, if security was considered by aides, logins may have been conducted from a secure network, such as those in place at U.S. diplomatic posts.

(U//~~FOUO~~) A disc with logins to CLINTON's account from April 18, 2009 to June 30, 2013, and IP address resolutions, is enclosed in a 1A envelope for the case file. A separate disc with the raw data obtained from OTD, dated June 17, 2016, is also enclosed.

♦♦

~~SECRET~~ // ~~NOFORN~~

HRC-8947

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1353814-0

Total Deleted Page(s) = 60

Page 3 ~ b1; b3; b6; b7C; b7E;
Page 4 ~ b1; b3; b6; b7C; b7E;
Page 5 ~ b1; b3; b6; b7C; b7E;
Page 6 ~ b1; b3; b7E;
Page 7 ~ b1; b3; b7E;
Page 8 ~ b1; b3; b7E;
Page 9 ~ b1; b3; b6; b7C; b7E;
Page 10 ~ b1; b3; b7E;
Page 11 ~ b1; b3; b7E;
Page 12 ~ b1; b3; b7E;
Page 13 ~ b1; b3; b7E;
Page 14 ~ b1; b3; b7E;
Page 15 ~ b1; b3; b7E;
Page 16 ~ b1; b3; b6; b7C; b7E;
Page 20 ~ b1; b3; b6; b7C; b7E;
Page 21 ~ b1; b3; b7E;
Page 22 ~ b1; b3; b6; b7C; b7E;
Page 23 ~ b1; b3; b6; b7C; b7E;
Page 24 ~ b1; b3; b6; b7C; b7E;
Page 25 ~ b1; b3; b6; b7C; b7E;
Page 26 ~ b1; b3; b6; b7C; b7E;
Page 27 ~ b1; b3; b6; b7C; b7E;
Page 28 ~ b1; b3; b7E;
Page 31 ~ Referral/Consult;
Page 33 ~ Referral/Consult;
Page 34 ~ Referral/Consult;
Page 35 ~ Referral/Consult;
Page 39 ~ b1; b3; b6; b7C; b7E;
Page 40 ~ b1; b3; b6; b7C; b7E;
Page 41 ~ b1; b3; b6; b7C; b7E;
Page 42 ~ b1; b3; b6; b7C; b7E;
Page 43 ~ b1; b3; b6; b7C; b7E;
Page 44 ~ b1; b3; b6; b7C; b7E;
Page 45 ~ b1; b3; b6; b7C; b7E;
Page 46 ~ b1; b3; b6; b7C; b7E;
Page 47 ~ b1; b3; b6; b7C; b7E;
Page 48 ~ b1; b3; b6; b7C; b7E;
Page 53 ~ b6; b7C; b7E;
Page 54 ~ b7E;
Page 55 ~ b7E;
Page 56 ~ b7E;
Page 57 ~ b7E;
Page 60 ~ b6; b7C; b7E;
Page 61 ~ b7E;
Page 62 ~ b7E;
Page 63 ~ b7E;
Page 64 ~ b7E;
Page 65 ~ b7E;

Page 66 ~ b7E;
Page 67 ~ b7E;
Page 68 ~ b7E;
Page 69 ~ b7E;
Page 70 ~ b7E;
Page 71 ~ b7E;
Page 72 ~ b7E;
Page 73 ~ b7E;
Page 74 ~ b7E;
Page 75 ~ b7E;
Page 76 ~ b7E;
Page 77 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

1A1

FD-340 (Rev 4-11-03)

File Number

[Redacted]

- 1A

b3
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document

[Redacted]

CYBER-3

Date Received

2/29/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

(CHICAGO)

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference: FD-1057 (EL) DATED 2/29/2016

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

ATTACHMENTS TO ANALYSIS EL FOR THE

[Redacted]

b7E

1A1

HRC-8970

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-19-2017 BY J76J18T80 NSICG

This is Google's cache of https://en.wikisource.org/wiki/Securing_Personal_E-mail_Accounts. It is a snapshot of the page as it appeared on Feb 9, 2016 06:09 16 GMT.

The current page could have changed in the meantime [Learn more](#)

[Full version](#) [Text-only version](#) [View source](#)

Tip: To quickly find your search term on this page, press **Ctrl+F** or **⌘-F** (Mac) and use the find bar.

Securing Personal E-mail Accounts

From Wikisource

Securing Personal E-mail Accounts

United States Department of State

United States Secretary of State Hillary Rodham Clinton

June 28, 2011

Securing Personal E-mail Accounts

Department of State
United States of America

MRN: 11 STATE 65111

Date/DTG: Jun 28, 2011 / 282223Z JUN 11

From: SECSTATE WASHDC

Action: ALL DIPLOMATIC AND CONSULAR POSTS COLLECTIVE ROUTINE

E.O.: 13526

TAGS: APCS, ASEC, AADP, AMGT

Subject: Securing Personal E-mail Accounts

UNCLAS STATE 065111

E.O. 13526: N/A

TAGS: APCS, ASEC, AADP, AMGT

SUBJECT: Securing Personal E-mail Accounts

Reference:

A) 12 FAM 544.3

1. Department of State users are encouraged to check the security settings and change passwords of their home e-mail accounts because of recent targeting of personal e-mail accounts by online adversaries. Security guidelines have been posted on the DS/SI/CS Cyber Security Awareness web page:

<http://intranet.ds.state.sbu/DS/SI/CS/Awareness1/Content/Personal%20Email.aspx>.

HRC-8985

2. Recently, Google asserted that online adversaries are targeting the personal Gmail accounts of U.S. government employees. Although the company believes it has taken appropriate steps to remediate identified activity, users should exercise caution and follow best practices in order to protect personal e-mail and prevent the compromise of government and personal information. The DS/SI/CS Cyber Security Awareness web site contains guides to help secure the web-based e-mail accounts of users and their families.

This information can be accessed at:

<http://intranet.ds.state.sbu/DS/SI/CS/Awareness1/Content/Personal%20Email.aspx>.

3. What can you and your family members do?
 - a. Follow the personal e-mail guides posted on the Awareness site to change your password, to ensure that messages are not auto-forwarding to an unintended address, and to verify that other security settings are properly configured.
 - b. Beware of e-mail messages that include links to password reset web pages. These can be easily faked.
 - c. Create strong passwords for all of your online accounts, change them often, and never use the same password for more than one account.
 - d. Avoid conducting official Department business from your personal e-mail accounts.
 - e. Do not reveal your personal e-mail address in your work "Out of Office" message.
 - f. Do not auto-forward Department e-mail to personal e-mail accounts, which is prohibited by Department policy (12 FAM 544.3).
4. Questions regarding cyber security awareness should be addressed to awareness@state.gov

CLINTON

Retrieved from "https://en.wikisource.org/w/index.php?title=Securing_Personal_E-mail_Accounts&oldid=5282193"



This work is in the **public domain** in the United States because it is a work of the United States federal government (see 17 U.S.C. 105).



Categories: 2011 works | PD-USGov | United States | Washington, D.C. | Communications | Internet
| United States Department of State | Computers

- This page was last modified on 9 March 2015, at 22:07.
- Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy.

#2

FD-340 (Rev 4-11-03)

File Number

[Redacted]

1A

b3
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document 4

Date Received 3/4/2016

From

SA

[Redacted]

(Name of Contributor/Interviewee)

b6
b7C

(Address)

(City and State)

By

SA

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

EC, DATED 03/04/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

[Redacted]

b6
b7C
b7E

ATTACHMENTS

HRC-8987

1A 3

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

-1A

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER-5

Date Received

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

(CYBER DIVISION)

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-1057, dated 3/9/16

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

DVD containing intelligence Bulletin summarizing
Email address research and analysis, in addition to
search results from FBI databases & iC3

1A3

HRC-8997

b3
b7E

b6
b7C

145

FD-340 (Rev. 4-11-03)

File Number

- 1A

b3
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document

7

Date Received 3/8/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes☒ No

Federal Taxpayer Information (FTI)

☐ Yes☒ No

Reference: FD-302 - DATED 3/8/2016

(Communication Enclosing Material)

Description: Original notes re interview of

SUPPORTING DOCUMENTATION FOR

ILCLOUD ANALYSIS.

LAS

HRC-9002

1A6

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

1A

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER- 8

Date Received

From

[Redacted]

(CYBER DIVISION)

(Name of Contributor/Interviewee)

b6
b7C

(Address)

(City and State)

By

[Redacted]

(CYBER DIVISION)

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-1057 (EC) dated 3/21/16

(Communication Enclosing Material)

Description:

☐ Original notes re interview of

Printout of spreadsheets of

[Redacted]

b7E

found in confirmed classified messages, as well
as a list of [Redacted] belonging to HRC's
close circle.

1A6

HRC-9003

1A7

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

CYBER

b3
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document

9

Date Received

3/9/2016

From

(Name of Contributor/Interviewee)

(Address)

By

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

SL DATED 3/9/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

[Redacted]

DEVELOPED FOR

CONFIRMED CLASSIFIED + CATEGORY 1

EMAILS.

b7E

1A7

HRC-9014

1A8

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

LYBER

b3
b7E

Field Office Acquiring Evidence

HQ/ WF

Serial # of Originating Document

60

Date Received

03/21/2016

From

TOU

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SFA

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

One (1) copy of TOU Report

One (1) ~~copy~~ of CD containing "Priv. master"

1A8

HRC-9015

1A9

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

CYBER

b3
b7E

Field Office Acquiring Evidence

HQ/WF

Serial # of Originating Document

11

Date Received

3/21/16

From

TOU

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SSA

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

One (1) TOU REPORT

One (1) LO with [Redacted] Report

b7E

1A9

HRC-9021

1A10

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

1A
~~1000~~

b3
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document 13, 14

Date Received 3/22/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference: EL - Dated 03/22/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

[Redacted]

SEARCH RESULTS

b7E

1A10

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1353814-0

Total Deleted Page(s) = 45

Page 7 ~ b6; b7C; b7E;
Page 8 ~ b7E;
Page 9 ~ b7E;
Page 10 ~ b6; b7C; b7E;
Page 11 ~ b7E;
Page 12 ~ b6; b7C; b7E;
Page 13 ~ b7E;
Page 14 ~ b7E;
Page 15 ~ b7E;
Page 16 ~ b7E;
Page 17 ~ b7E;
Page 18 ~ b7E;
Page 22 ~ b1; b3; b7E;
Page 26 ~ b3; b6; b7C; b7E;
Page 27 ~ b3; b6; b7C; b7E;
Page 28 ~ b3; b6; b7C; b7E;
Page 29 ~ b3; b6; b7C; b7E;
Page 31 ~ b1; b3; b6; b7C; b7E;
Page 32 ~ b3; b6; b7C; b7E;
Page 54 ~ b6; b7C;
Page 78 ~ b7E;
Page 79 ~ b7E;
Page 80 ~ b7E;
Page 81 ~ b7E;
Page 82 ~ b7E;
Page 83 ~ b7E;
Page 84 ~ b7E;
Page 85 ~ b7E;
Page 89 ~ b7E;
Page 90 ~ b6; b7C; b7E;
Page 91 ~ b6; b7C; b7E;
Page 92 ~ b6; b7C; b7E;
Page 93 ~ b6; b7C; b7E;
Page 94 ~ b6; b7C; b7E;
Page 95 ~ b6; b7C; b7E;
Page 96 ~ b6; b7C; b7E;
Page 97 ~ b6; b7C; b7E;
Page 98 ~ b6; b7C; b7E;
Page 99 ~ b7E;
Page 100 ~ b6; b7C; b7E;
Page 101 ~ b6; b7C; b7E;
Page 102 ~ b6; b7C; b7E;
Page 103 ~ b7E;
Page 104 ~ b6; b7C; b7E;
Page 105 ~ b7E;

XXXXXXXXXXXXXXXXXXXXXXXXXXXXX

X Deleted Page(s) X

X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXXXXXXX

~~SECRET~~

CLASSIFIED BY: NSICG J76J18780
REASON: 1.4 (C)
DECLASSIFY ON 12-31-2041
DATE: 01-19-2017

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED EXCEPT
WHERE SHOWN OTHERWISE

1A11

FD-340 (Rev 4-11-03)

File Number

[Redacted] -1A

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER-15

Date Received

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

(CYD)

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (c)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-1057 dated 3/22/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

Research and analysis results related to

[Redacted]

identified email accounts and the

(S)

Clintonemail.com domain.

b1
b3
b7E

1A11

HRC-9041

~~SECRET~~

1A12

FD-340 (Rev 4-11-03)

File Number

[Redacted] - 1A

b3
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document 16

Date Received 3/23/2016

From

[Redacted]

(Name of Contributor/Interviewee)

[Redacted]

(Address)

b6
b7C

[Redacted]

(City and State)

By

SA [Redacted]

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-302 -

[Redacted]

(Communication Enclosing Material)

b6
b7C

Description:

☒ Original notes re interview of

[Redacted]

[Redacted]

INTERVIEW NOTES

b6
b7C

1A12

HRC-9042

b4

- Not live today - Verizon IP

- Leaky, Meule

b6

b7C

b4

b4

- No logs on who adds assets.

- Not able to trace

- HC not active in their system today.

- Likely good-guy activity searching for public information
chan-up

- snap-shot of what's out there / On-going monitoring.

- Media company clients

~~SECRET//NOFORN~~

1A13

FD-340 (Rev 4-11-03)

File Number

CYBER

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

17

Date Received

2/10/2016

From

IAU

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

ITS/FE

To Be Returned

☐ Yes

☒ No

Receipt Given

☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

(U)

~~(S//NF)~~ MIDYER EXAM,
MISHANDLING OF CLASSIFIED,
UNKNOWN SUBJECT OR COUNTRY
SENSITIVE INVESTIGATIVE MATTER (SIM)

Reference:

CART, Serial-3

(Communication Enclosing Material)

Description:

☒ Original notes re interview of MC

Copy of final technical analysis report
from IAU - 12 pages

1A13

~~SECRET//NOFORN~~

HRC-9044

b3
b7E

b6
b7C

b6
b7C

b3
b7E

1A14

FD-340 (Rev 4-11-03)

File Number

[Redacted]

1A

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

19

Date Received

3/24/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

[Redacted]

/ 1A

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

EC - DATED 03/24/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

SUPPORTING DOCUMENTATION FOR
FD ANALYSIS

HRC-9057

1A14

1A15

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

1A

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER - 20

Date Received

3/24/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

(CYD)

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-1057 dated 3/24/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

printout of the

[Redacted]

results for IP address

[Redacted]

b6
b7C
b7E

1A15

HRC-9058

1A16

FD-340 (Rev 4-11-03)

File Number

[Redacted]

1A

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER-21

Date Received

3/28/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

(CYD)

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-1057 dated 3/28/2016

(Communication Enclosing Material)

Description:

☐ Original notes re interview of

search results for email addresses in new
confirmed classified not previously identified, and
two other accounts part of the original group
of classified messages.

1A16

HRC-9060

b3
b7E

b6
b7C

FD-340 (Rev 4-11-03)

File Number

1A17
[Redacted] 1A

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted] CYBER-22

Date Received

03/31/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted] (CYD)

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-1057 dated 03/31/2016

(Communication Enclosing Material)

Description:

☐ Original notes re interview of

Subpoena returns for

[Redacted]

1A17

HRC-9061

b3
b7E

b6
b7C

b3
b6
b7C
b7E

1A18

FD-340 (Rev 4-11-03)

File Number

[Redacted]

1A

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER-25

Date Received

4/8/16

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

(CYD)

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-1057 dated 04/8/16

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

Printout of Excel spreadsheet listing
device identifiers.

1A18

1A19

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

CYBER

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

26

Date Received

4/12/2016

From

[Redacted]

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

[Redacted]

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

Reference:

FD-302 - Dated 4/14/2016 -

[Redacted]

(Communication Enclosing Material)

Description:

☒

Original notes re interview of

[Redacted]

EMAILS PROVIDED BY

[Redacted]

1A19

HRC-9069

b3
b7E

b6
b7C

b6
b7C

b6
b7C

~~SECRET~~

1 - Confidentiality Statement

- 2:00 PM

- [redacted]
- 4/12/16

[redacted]

- 6 months - before media

b6
b7C

IR - MNCs - asked

Take Talent for IR - Fravall + vice versa

Business Relationship

[redacted]

story coming out

[redacted]

- NO

b1
b3

PRN - name comes

b6
b7A

TELEMS exchanged calls

Did not do work on

b7C
b7E

hit news shortly after that

[redacted]

fravall -

emails / shared access

Payments - commission checks back + forth

Subsequent to PRN hitting - Recommend PRN

b6
b7C

-

[redacted]

- Leads group

- 15 companies

No schemes at PRN. -

- Colviado

Willing to cooperate but asked - Doesn't talk regularly

Tech
hunting

Good guy - Got fucked in this whole deal

- Small Business

[redacted]

- Secret Source - + the Platt River

implied -

Not sure

Asked to step out of RFPs - served warrant on source.

[redacted]

b6
b7C

Another million in legal fees.

[redacted]

b6
b7C

[redacted]

FBI INFO.

CLASSIFIED BY: NSICG J37J85T94

REASON: 1.4 (C)

DECLASSIFY ON: 12-31-2041

DATE: 03-06-2018

- 2004 - ant-dial

~~SECRET~~

HRC-9070

~~SECRET~~

- 8/31 - ATTC Email

- 3/11/2015 - Media Email DIDN'T HAPPEN

Follow-up call to SA [] - served warrant

[] - Platte Rivera

b3
b6
b7C
b7E

- Separate matter / unrelated to ATTC.

[] - USSS - 3:15 PM

b6
b7C

[] is upset by media ^{reports} + this situation

~~SECRET~~

HRC-9071

4/12/16

Ever do pen testing for PRN around 3/2015?

Who contacted them? Scope of job?

Did they ever have access to data on the server?

Does [redacted] use [redacted] social media tools

b6

b7C

Which [redacted] employees performed the pen testing?

b7E

Can we have associated paperwork?

Are there any other relationships w/ PRN?

What tools were used for the pen testing? Keyloggers/malware?

How long did the project last?

What were the security recommendations to PRN?

Did [redacted] ever interact with CESC?

b6

b7C

b7E

b6
b7C

[REDACTED]

From: [REDACTED]
Sent: Thursday, February 18, 2016 5:29 PM
To: [REDACTED]
Subject: RE: Optiv

Cool. Thanks., Someone looking to work there and was concerned.

b6
b7C



We build better networks... Because your business depends on IT.

From: [REDACTED]
Sent: Thursday, February 18, 2016 4:18 PM
To: [REDACTED]
Subject: RE: Optiv

b6
b7C

Fishnet used to be a smallish shop out of Kansas City, which grew to 500+ head count over the years, and prior to the merger. A lot of the tech talent and leadership bounced because their culture was now colonized by big corporate. Beyond that, I've not heard of any issues other than what you would expect from a merger... integration issues (with systems, processes, and culture). We have never done any work with them from a partner standpoint.

From: [REDACTED]
Sent: Thursday, February 18, 2016 4:11 PM
To: [REDACTED]
Subject: RE: Optiv

b6
b7C

Since their merger last year I'm hearing they are having lots of problems.
Do you run into them ever?

b6
b7C



We build better networks... Because your business depends on IT.

HRC-9073

From: [REDACTED]
Sent: Thursday, February 18, 2016 4:06 PM
To: [REDACTED]
Subject: RE: Optiv

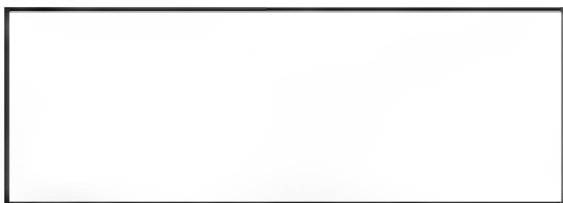
b6
b7C

Not sure what you are referencing...

From: [REDACTED]
Sent: Thursday, February 18, 2016 3:45 PM
To: [REDACTED]
Subject: Optiv

b6
b7C

What's up with Optiv? Are they tanking? What are you seeing?



b6
b7C



We build better networks. Because your business depends on it.



b6
b7C

[REDACTED]

From: [REDACTED]
Sent: Tuesday, February 02, 2016 9:06 PM
To: [REDACTED]
Subject: FW: SnowFROC 2016 conference
Attachments: SnowFROC16Promo.pptx

See attached and below. Thought you might be interested.

b6
b7C



We build better networks... Because your business depends on IT.

From: [REDACTED]
Sent: Tuesday, February 02, 2016 7:10 PM
To: [REDACTED]
Subject: SnowFROC 2016 conference

b6
b7C

Hi [REDACTED]

Attached is info on the conference I'm putting on Feb 18th. It is at SecureSet. 3801 Franklin Street, Denver 80205.

If you know anyone who wants to sponsor that would be great. I've attached the sponsor forms and a slide with the info on it.

Let me know if you want to come and I'll print up a complimentary badge for you.

Thanks!!



b6
b7C



b6
b7C

HRC-9075

b6
b7C

[REDACTED]

From: [REDACTED]
Sent: Tuesday, December 08, 2015 10:10 AM
To: [REDACTED]
Subject: RE: URGENT - spoofed email and wire...

Hi [REDACTED]

b6
b7C

This is a common attack scenario. I'm a slow typer, but free to catch up by phone to discuss. I am free today from 11:30-2, or after 4:30 for a call. Please feel free to call whenever you have a moment.

[REDACTED]

[REDACTED]

b6
b7C

From: [REDACTED]
Sent: Tuesday, December 08, 2015 9:28 AM
To: [REDACTED]
Subject: URGENT - spoofed email and wire...

b6
b7C

[REDACTED]

Our client had an internal exec email spoofed and causing an inadvertent \$25K wire going out.

Can we ask for your advice on how to keep this from happening in the future.

I have copied [REDACTED] and [REDACTED] who are working on this for the client. Have you seen this before?

b6
b7C

What do you recommend?

Thanks!

[REDACTED]

b6
b7C



We build better networks... Because your business depends on IT.

HRC-9076



b6
b7c

b6
b7C

[REDACTED]

From: [REDACTED]
Sent: Monday, August 31, 2015 2:14 PM
To: [REDACTED]
Subject: RE: Thoughts??

Finally quieted down once our Publicists got the facts out.

Expect it to flare up a few more times than disappear. Yay!

b6
b7C



From: [REDACTED]
Sent: Monday, August 31, 2015 2:04 PM
To: [REDACTED]
Subject: RE: Thoughts??

b6
b7C

We may throw something together. Debating if we can pull it off. How's the media shit storm treating you?

From: [REDACTED]
Sent: Monday, August 31, 2015 12:20 PM
To: [REDACTED]
Subject: FW: Thoughts??

b6
b7C



b6
b7C

HRC-9078

From: [REDACTED]
Sent: Monday, August 31, 2015 10:50 AM
To: [REDACTED]
Subject: Thoughts??

b6
b7C

Not a whole lot of time.... RFP due Sept 3rd ☹



b6
b7C



b6
b7C

b6
b7C

[REDACTED]

From: [REDACTED]
Sent: Saturday, May 02, 2015 1:32 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: Re: Risk Assessment

Perfect
Thx

Sent from my iPhone

On May 2, 2015, at 2:48 PM [REDACTED] wrote:

b6
b7C

Thanks for the email [REDACTED] He left me a voicemail on Friday but I was traveling all day. I am planning on calling him on Monday. We routinely do risk assessments for our clients cyber reach insurance underwriting. Will keep you posted.

Thanks,

On May 2, 2015, at 11:48 AM, [REDACTED] wrote:

b6
b7C

Hi [REDACTED]

Please see below. Can we make an introduction?

From: [REDACTED]
Sent: Friday, May 01, 2015 12:54 PM
To: [REDACTED]
Cc: CRC
Subject: Risk Assessment

b6
b7C

Hey guys – not sure where to go with this one. Just got a call from [REDACTED] there are a CPA Firm downtown. They are looking into getting Cyber Insurance and in order to do this they need a risk assessment done on their network by someone other than their in house IT guy. They have 50 users.

b6
b7C

He was referred to us by the ALA and remembers meeting [REDACTED] about 3 years ago.

[REDACTED]

[REDACTED]

b6
b7C

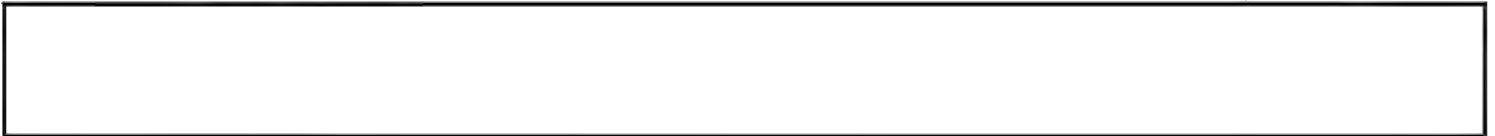
<image001.jpg>

HRC-9080



b6
b7c

<image001.jpg>





b6
b7C

Re Clinton email

7 messages

[Redacted]
To: [Redacted] Wed, Mar 11, 2015 at 10:13 AM

Hi! It's [Redacted] Wondering if u might be available for a live telephone interview this Saturday morning for our KNUS radio show. Want to talk about Hillary Clinton having own server from a cyber security point of view. We r thinking 8 am.
My cell is [Redacted] Thx!
Sent from my iPhone

b6
b7C

[Redacted]
To: [Redacted] Wed, Mar 11, 2015 at 12:53 PM

Hey [Redacted] I never miss the opportunity for a media appearance, But I think I'll definitely take a pass on this one. LOL



b6
b7C

Begin forwarded message:

From: [Redacted]
Date: March 11, 2015 at 10:13:43 AM MDT
To: [Redacted]
Subject: Re Clinton email

b6
b7C

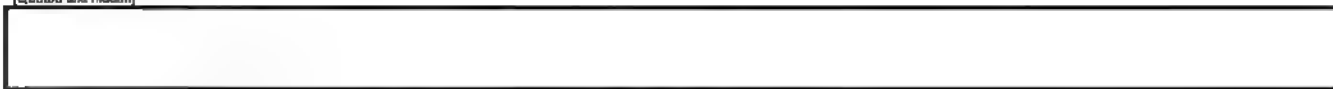
Hi! It's [Redacted] Wondering if u might be available for a live telephone interview this Saturday morning for our KNUS radio show. Want to talk about Hillary Clinton having own server from a cyber security point of view. We r thinking 8 am.
My cell is [Redacted] Thx!
Sent from my iPhone

[Redacted]
To: [Redacted] Wed, Mar 11, 2015 at 12:54 PM

b6
b7C

Too funny
Thanks for passing

Sent from my iPhone
[Quoted text hidden]



[Redacted]
To: [Redacted] Wed, Mar 11, 2015 at 12:55 PM

Hi [Redacted] thanks for reaching out to us but I will be out of the country until March 25, and will not be available in the meantime. Please keep in touch in the future as I truly appreciate the offer.

Thanks [Redacted]



b6
b7C

[Quoted text hidden]

[Redacted]
To: [Redacted] Wed, Mar 11, 2015 at 2:52 PM

b6
b7C

HRC-9082

Thanks and enjoy your trip.

Is there anyone else with your company that you could recommend?

Thanks,

[Redacted]
[Quoted text hidden]

Thu, Mar 12, 2015 at 8:45 AM

To: [Redacted]

b6
b7C

SecurityWeek.Com
www.securityweek.com/clinton-email-server-vulnerable-3-months-venafi

[Redacted]

[Quoted text hidden]

b6
b7C

Fri, Mar 13, 2015 at 9:27 AM

To: [Redacted]

Good thing we did not take over until after she left office in July of 2013

From: [Redacted]
Sent: Thursday, March 12, 2015 7:46 AM
To: [Redacted]
Subject: Re: Re Clinton email

[Quoted text hidden]
[Quoted text hidden]

b6
b7C



b6
b7C

FW: clinton's - please read - do we need to make these changes recommended?
7 messages

To: [Redacted]
Cc: [Redacted]

Sat, Mar 7, 2015 at 4:18 PM

b6
b7C

Hi [Redacted]

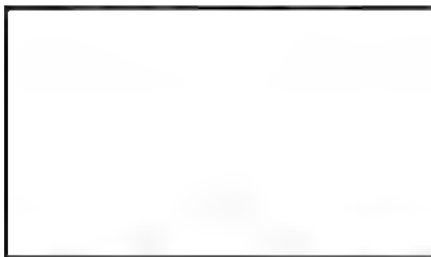
Please read article below regarding cert for the Clinton's Fortinet firewall

Our techs copied here have [Redacted]

b4
b6
b7C

Is this sufficient? [Redacted] is working on this now.

THANKS



b6
b7C



From: [Redacted]
Sent: Saturday, March 07, 2015 12:14 PM
To: [Redacted]
Cc: [Redacted]
Subject: RE: clinton's - please read - do we need to make these changes recommended?

b6
b7C

This only affects remote logins [Redacted] and nothing to do with the email/email server.

b4
b6
b7C

That being said, we may want to [Redacted] altogether. What do you think [Redacted] We would just need to [Redacted] to manage it.

From: [Redacted]
Sent: Saturday, March 7, 2015 1:22 PM
To: [Redacted]
Cc: [Redacted]
Subject: clinton's - please read - do we need to make these changes recommended?

b6
b7C

Clinton's top aide during that period, Cheryl Mills, is a respected scandal-defense lawyer. As a member of the White House counsel's office, Mills helped guide President Bill Clinton through a series of investigations in the 1990s and won praise for her performance in successfully defending him when the Senate voted not to remove him from office in

HRC-9084

1999.

Mills would go on to combine two of the most powerful posts at the State Department -- chief of staff and counselor -- under Hillary Clinton. In that job, she spoke for Clinton on management matters within the department.

Mills didn't reply to an e-mail seeking comment.

Not long after resigning as secretary of state, Clinton's private e-mail service was transferred to a commercial provider, MX Logic, Devost said.

"The timing makes sense," Devost said. "When she left office and was no longer worried as much about control over her e-mails, she moved to a system that was easier to administer."

It took less than a day for researchers to find potential problems with the Clinton's system.

Using a scanning tool called Fierce that he developed, Robert Hansen, a web-application security specialist, found what he said were the addresses for Microsoft Outlook Web access server used by Clinton's e-mail service, and the virtual private network used to download e-mail over an encrypted connection. If hackers located those links, they could search for weaknesses and intercept traffic, according to security experts.

Factory Default

Using those addresses, McGeorge discovered that the certificate appearing on the site Tuesday appeared to be the factory default for the security appliance, made by Fortinet Inc., running the service.

Those defaults would normally be replaced by a unique certificate purchased for a few hundred dollars. By not taking that step, the system was vulnerable to hacking.

It's unclear whether the site's settings were the same before news of the private e-mail account emerged this week.

Fortinet issued a statement saying it wasn't aware the company's technologies were used by Clinton.

"If they were, our recommendation is to replace provided self-signed certificates with valid digital certificates for the protected domains," said Andrea Cousens, a Fortinet spokeswoman.

"It may have fallen in the realm of acceptable risk," Devost said. "They wanted to make sure that when she was in Egypt all of the traffic from her phone to the mail server was encrypted and that was their priority."

To contact the reporters on this story: Michael Riley in Washington at michaelriley@bloomberg.net; Jordan Robertson in Washington at jrobertson40@bloomberg.net; Chris Strohm in Washington at cstrohm1@bloomberg.net

[Redacted]

b6
b7C

Sat, Mar 7, 2015 at 8:14 PM

To: [Redacted]
Cc: [Redacted]

H [Redacted] and [Redacted]

Please feel free to give me a call anytime at [Redacted] if I can help in anyway.

Thanks [Redacted]

b6
b7C

[Redacted]

On Mar 7 2015, at 4:16 PM, [Redacted] wrote:

b6
b7C

H [Redacted]

Please read article below regarding cert for the Clinton's Fortinet firewall

Our techs copied here have [Redacted]

b4
b6
b7C

Is this sufficient? [Redacted] is working on this now.

THANKS

b6
b7C

[Redacted]

<image001.jpg>

[Quoted text hidden]

[Quoted text hidden]

Sat, Mar 7 2015 at 8:16 PM

To: [Redacted]
Cc: [Redacted]

How about now? If not, it can wait for Monday. .

[Redacted]

b6
b7C

HRC-9086

[Redacted]

b6
b7C

From: [Redacted]
Date: Saturday, March 7, 2015 at 8:14 PM
To: [Redacted]
Cc: [Redacted]
Subject: Re: clinton's - please read - do we need to make these changes recommended?
[Quoted text hidden]
[Quoted text hidden]

b6
b7C

[Redacted]
To: [Redacted]
Cc: [Redacted]
Sat, Mar 7, 2015 at 8:18 PM

b6
b7C

[Redacted] know you have a gig tonight when you get a chance tomorrow hopefully can you respond to the emails as far as suggestions and then maybe we can set up a call with you [Redacted] and [Redacted] for Monday

Sent from my iPhone
[Quoted text hidden]

[Redacted]
To: [Redacted]
Cc: [Redacted]
Sat, Mar 7, 2015 at 8:40 PM

b6
b7C

[Redacted] is performing tonight

Sent from my iPhone

On Mar 7, 2015, at 8:16 PM [Redacted] wrote:

How about now? If not, it can wait for Monday

b6
b7C

[Redacted]

PLATTE RIVER NETWORKS
IT SERVICES FOR BUSINESS

[Redacted]

[Quoted text hidden]

[Quoted text hidden]

2 attachments

[Redacted]

b6
b7C

[Redacted]
To: [Redacted]
Cc: [Redacted]
Sat, Mar 7, 2015 at 8:44 PM

No worries. I am still at the office, so figured I'd try. It can wait for Monday. I put the [Redacted] I guess we could [Redacted] if we are certain [Redacted]

b4
b6
b7C

[Redacted]

[Redacted]

b6
b7C

From: [Redacted]

Date: Saturday, March 7, 2015 at 8:40 PM

To: [Redacted]

Cc: [Redacted]

[Quoted text hidden]

[Quoted text hidden]

[Quoted text hidden]

b6
b7C

[Redacted]

Sat, Mar 7, 2015 at 11:54 PM

b6
b7C

To: [Redacted]

Cc: [Redacted]

I'm available now, or anytime over the weekend if you would like to touch base. Feel free to call anytime.

[Redacted]

b6
b7C

On Mar 7, 2015, at 8:44 PM, [Redacted] wrote:

No worries, I am still at the office, so figured I'd try. It can wait for Monday. I put the [Redacted]
guess we could [Redacted] if we are certain [Redacted]

b4



PLATTE RIVER NETWORKS

IT SERVICES FOR BUSINESS

b6
b7C

[Quoted text hidden]



Recommendations for additional Cyber Security...

1 message

Sat, Mar 7, 2015 at 12:55 PM

To: [redacted]
Cc: [redacted]

b6
b7C

Thanks [redacted]

b6
b7C

I have copied [redacted] and [redacted] on our end who may have questions.

thanks



b6
b7C



From: [redacted]
Sent: Thursday, March 05, 2015 4:01 PM
To: [redacted]
Subject: Quick Thoughts

b6
b7C

Hi [redacted]

Some quick thoughts on shoring up the defenses. The most likely scenario to play out would be your staff targeted with a phishing email, to either ask them for credentials to the local network, or asking them to click a link, which will install malware. Once malware is installed, keystrokes are logged to capture the LAN credentials. So we would definitely recommend an all-hands refresher ASAP on security awareness / social engineering vigilance.

As for technical controls:

- Implement 0-day protection on the perimeter (url filtering and malware sandboxing)
- Monitor all access and failed attempts to access your network resources, and your client's resources.
- Conduct vulnerability scanning on your network to verify that patching was effective, should someone click the link.
- You may also want to put any admins who work on the clients account, into their own isolated vlan, should one of the other Platte River employees get infected/compromised.
- Confirm all vectors of access into the environments.

Let me know if you would like to touch base by phone to discuss further

[redacted]

[redacted]

b6
b7C

HRC-9089

#20

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

CYBER-1A

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER-27

Date Received

05/11/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[Redacted]

(CYD)

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A20

Reference:

FD-1057 dated 05/11/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

Disc containing Attack ID descriptions and
associated IP addresses, along with research
results.

HRC-9091

#21

FD-340 (Rev 4-11-03)

File Number

[REDACTED]

-CYBER-1A-

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[REDACTED]

-CYBER-29

Date Received

05/17/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

[REDACTED]

(CYD)

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A21

Reference:

FD-1057 dated 05/17/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

Two discs

[REDACTED]

of Blumenthal memos and

[REDACTED]

of known classified memos. Also included

is confirmation of

[REDACTED]

in the Guccifer Archive,

and a fact sheet printed from hillaryclinton.com

HRC-9092

b3
b7E

b6
b7C

b7E

THE BRIEFING

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-20-2017 BY J76J18T80 NSICG

The Briefing

Factsheets

Updated: The Facts About Hillary Clinton's Emails

We've put all of the information about Hillary Clinton's State Department emails here. Just the facts, all in one place.

Why did Clinton use her own email account?

When Clinton got to the Department, she opted to use her personal email account as a matter of convenience. It enabled her to reach people quickly and keep in regular touch with her family and friends more easily given her travel schedule.

That is the only reason she used her own account.

Her usage was widely known to the over 100 State Department and U.S. government colleagues she emailed, consistent with the practice of prior Secretaries of State and permitted at the time.

As Clinton has said, in hindsight, it would have been better to just have two accounts. While she thought using one account would be easier, obviously, that has not been the case.

Was it allowed?

Yes. The laws, regulations, and State Department policy in place during her tenure permitted her to use a non-government email for work.

The 2009 National Archives regulation in place during her tenure required that "[a]gencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system." The regulation recognizes the use of non-government email accounts.

As she has stated, Clinton's practice was to email government officials on their ".gov" accounts, so her work emails were immediately captured and preserved. In fact, more than 90% of those emails should have already been captured in the State Department's email system before she provided them with paper copies.

A Politifact analysis also confirmed that Clinton's practices complied with laws and regulations, including support from the former director of a prominent government accountability organization: "In Clinton's defense, we should note that it was only after Clinton left the State Department, that the National Archives issued a recommendation that government employees should avoid conducting official business on personal emails (though they noted there might be extenuating circumstances such as an emergency that require it). Additionally, in 2014, President Barack Obama signed changes to the Federal Records Act that explicitly said federal officials can only use personal email addresses if they also copy or send the emails to their official account. Because these rules weren't in effect when Clinton was in office, 'she was in compliance with the laws and regulations at the time,' said Gary Bass, founder and former director of OMB Watch, a government accountability organization."

Clinton said she did not use her email to send or receive classified information, but the State Department and two Inspectors General said some of these emails do contain classified information. Was her statement inaccurate?

Clinton only used her account for unclassified email. No information in Clinton's emails was marked classified at the time she sent or received them.

When information is reviewed for public release, it is common for information previously unclassified to be upgraded to classified if the State Department or another agency believes its public release could cause potential harm to national security, law enforcement or diplomatic relations.

After reviewing a sampling of the 55,000 pages of emails, the Inspectors General have proffered that a small number of emails, which did not contain any classified markings and/or dissemination controls, should have been classified at the time they were sent. The State Department has said it disagrees with this assessment.

Clinton hopes the State Department and the agencies involved in the review process will sort out as quickly as possible which of the 55,000 pages of emails are appropriate to share with the public.

How did Clinton receive and consume classified information?

The Secretary's office was located in a secure area. Classified information was viewed in hard copy by Clinton while in the office. While on travel, the State Department had rigorous protocols for her and traveling staff to receive and transmit information of all types.

A separate, closed email system was used by the State Department for the purpose of handling classified communications, which was designed to prevent such information from being transmitted anywhere other than within that system.

Is Department of Justice conducting a criminal inquiry into Clinton's email use?

No. As the Department of Justice and Inspectors General made clear, the IGs made a security referral. This was not criminal in nature as misreported by some in the press. The Department of Justice is now seeking assurances about the storage of materials related to Clinton's email account.

Is it true that her email server and a thumb drive were recently turned over to the government? Why?

Again, when information is reviewed for public release, it is common for information previously unclassified to be upgraded to classified if the State Department or another agency believes its public release could cause potential harm to national security, law enforcement or diplomatic relations.

Clinton hopes that State and the other agencies involved in the review process will sort out as quickly as possible which emails are appropriate to share with the public, and that the release will be as timely and as transparent as possible.

When the Department upgraded some of the previously unclassified email to classified, her team worked with the State Department to ensure copies of her emails were stored in a safe and secure manner. She also directed her team to give her server that hosted her email account while she was Secretary to the Department of Justice, as well as a thumb drive containing copies of her emails that already had been provided to the State Department. Clinton has pledged to cooperate with the government's security inquiry.

Would this issue not have arisen if she used a state.gov email address?

Even if Clinton's emails had been on a government email address and government device, these questions would be raised prior to public release.

While the State Department's review of her 55,000 emails brought the issue to the Inspectors General's attentions, the emails that recently were upgraded to classified prior to public release were on the unclassified .gov email system. They were not on the separate, closed system used by State Department for handling classified communications.

Have Clinton's State Department aides also been asked to provide the Department and Congress with emails from their personal accounts?

We understand that members of her State Department staff were recently asked to assist the Department in its record-keeping by providing any work-related emails they may have on personal accounts. They have received requests from Rep. Gowdy as well.

Clinton is proud of the work of all the dedicated public servants that were part of her team at the State Department. She was proud of her aides then and is proud of them now, as they have committed - as she has - to being as helpful as possible in responding to requests.

Press reports say she used multiple devices - a Blackberry and an iPad - is that true?

Clinton relied on her Blackberry for emailing. This was easiest for her. When the iPad came out in 2010, she was as curious as others and found it great for shopping, browsing, and reading articles when she traveled. She also had access to her email account on her iPad and sometimes used it for that too.

Was she ever provided guidance about her use of a non-".gov" email account?

The State Department has and did provide guidance regarding the need to preserve federal records. To address these requirements, it was her practice to email government employees on their ".gov" email address. That way, work emails would be immediately captured and preserved in government record-keeping systems.

What did Clinton provide to the State Department?

On December 5, 2014, 30,490 copies of work or potentially work-related emails sent and received by Clinton from March 18, 2009, to February 1, 2013, were provided to the State Department. This totaled roughly 55,000 pages. More than 90% of her work or potentially work-related emails provided to the Department were already in the State Department's record-keeping system because those e-mails were sent to or received by "state.gov" accounts.

Early in her term, Clinton continued using an att.blackberry.net account that she had used during her Senate service. Given her practice from the beginning of emailing State Department officials on their state.gov accounts, her work-related emails during these initial weeks would have been captured and preserved in the State Department's record-keeping system. She, however, no longer had access to these emails once she transitioned from this account.

Why did the Select Committee announce that she used multiple email addresses during her tenure?

In fairness to the Committee, this was an honest misunderstanding. Clinton used one email account during her tenure at State (with the exception of her initial weeks in office while transitioning from an email account she had previously used). In March 2013, a month after she left the Department, Gawker published the email address she used while Secretary, and so she had to change the address on her account.

At the time the printed copies were provided to the Department in 2014, because it was the same account, the new email address established after she left office appeared on the printed copies as the sender, and not the address she used as Secretary. In fact, this address on the account did not exist until March 2013. This led to understandable confusion that was cleared up directly with the Committee after its press conference.

Why didn't Clinton provide her emails to the State Department until December 2014?

In 2014, after recognizing potential gaps in its overall recordkeeping system, the State Department asked for the help of the four previous former Secretaries in meeting the State Department's obligations under the Federal Records Act.

Clinton responded to this request by providing the State Department with over 55,000 pages of emails. As it was Clinton's practice to email U.S. government officials on their .gov accounts, the overwhelming majority of these emails should have already been preserved in the State Department's email system.

In providing these emails to the Department, Clinton included all she had that were even potentially work-related—including emails about using a fax machine or asking for iced tea during a meeting—errring on the side of over-inclusion, as confirmed by the Department and National Archives' determination that over 1250 emails were "personal" records (which they have indicated will be returned to her).

After providing her work and potentially work-related emails, she chose not to keep her personal, non-work related emails, which by definition, are not federal records and were not requested by the Department or anyone else.

Why did the State Department ask for assistance in collecting records? Why did the State Department need assistance in further meeting its requirements under the Federal Records Act?

The State Department formally requested the assistance of the four previous former Secretaries in a letter to their representatives dated October 28, 2014, to help in further meeting the Department's requirements under the Federal Records Act.

The letter stated that in September 2013, the National Archives and Records Administration (NARA) issued new guidance clarifying records management responsibilities regarding the use of personal email accounts for government business.

While this guidance was issued after all four former Secretaries had departed office, the Department decided to ensure its records were as complete as possible and sought copies of work emails sent or received by the Secretaries on their own accounts.

Why did Clinton decide not to keep her personal emails?

As Clinton has said before, these were private, personal messages, including emails about her daughter's wedding plans, her mother's funeral services and condolence notes, as well as emails on family vacations, yoga routines, and other items one would typically find in their own email account, such as offers from retailers, spam, etc.

Did Clinton delete any emails while facing a subpoena?

No. As noted, the emails that Clinton chose not to keep were personal emails—they were not federal records or even work-related—and therefore were not subject to any preservation obligation under the Federal Records Act or any request. Nor would they have been subject to the subpoena—which did not exist at the time—that was issued by the Benghazi Select Committee some three months later.

Rep. Gowdy's subpoena issued in March 2015 did not seek, and had nothing to do with, her personal, non-work emails nor her server nor the request by State Department last year for her help in their own record-keeping. Indeed in his March 19th letter, Rep. Gowdy expressly stated he was not seeking any emails that were "purely personal in nature."

In March 2015, when Rep. Gowdy issued a subpoena to Clinton, the State Department had received all of Clinton's work-related emails in response to their 2014 request, and indeed, had already provided Clinton's relevant emails to Rep. Gowdy's committee.

Rep. Gowdy, other Republicans, and some members of the media have seized on a CNN interview with Clinton to question her on this point. Rep. Gowdy has even gone so far as to say Clinton is lying. But he and the others are clearly mistaken.

As Vox reported, "[S]he didn't lie about the subpoena. ... Clinton clearly wasn't responding to the question of whether she'd ever been subpoenaed by the Benghazi Committee but whether she'd been subpoenaed before she wiped the emails from her server." Additionally, Factcheck.org said in its analysis, "Clinton's denial came in response to a question about deleting emails 'while facing a subpoena,' and Clinton objected to Keilar's 'assumption.' Clinton's campaign said that the emails were deleted before she received the subpoena and that was the point Clinton was making." Politifact added, "Suggesting that Clinton deleted emails while facing a subpoena contradicts what we know about the controversy so far."

Vox went on to further decry Rep. Gowdy's reaction, saying, "[T]his one's a particularly absurd gimmick, even for a committee that is selectively leaking from depositions and documents to justify its existence. If there was a more extreme category of dissembling than 'pants on fire,' now would be the time for Politifact to roll it out on the House Republicans."

Why was the State Department given printed copies?

That is the requirement. The instructions regarding electronic mail in the Foreign Affairs Manual (the Department's policy manual) require that "until technology allowing archival capabilities for long-term electronic storage and retrieval of email messages is available and installed, those messages warranting preservation as records (for periods longer than current E-mail systems routinely maintain them) must be printed out and filed with related records." [5 FAM 443.3].

Were any work items deleted in the course of producing the printed copies?

No.

How many emails were in her account? And how many of those were provided to the State Department?

Her email account contained a total of 62,320 sent and received emails from March 2009 to February 2013. Based on the review process described below, 30,490 of these emails were provided to the Department, and the remaining 31,830 were private, personal records.

How and who decided what should be provided to the State Department?

The Federal Records Act puts the obligation on the government official to determine what is and is not a federal record. The State Department Foreign Affairs Manual outlines guidance "designed to help employees determine which of their e-mail messages must be preserved as federal records and which may be deleted without further authorization because they are not Federal record materials." [5 FAM 443.1(c)].

Following conversations with State Department officials and in response to the State Department's 2014 letter to former Secretaries, Clinton directed her attorneys to assist by identifying and preserving all emails that could potentially be federal records. This entailed a multi-step process to review each email and provide printed copies of Clinton's emails to the State Department, erring on the side of including anything that might be even potentially work-related.

A search was conducted on Clinton's email account for all emails sent and received from 2009 to her last day in office, February 1, 2013.

After this universe was determined, a search was conducted for a ".gov" (not just state.gov) in any address field in an email. This produced over 27,500 emails, representing more than 90% of the 30,490 printed copies that were provided to the State Department.

To help identify any potential non-".gov" correspondence that should be included, a search of first and last names of more than 100 State Department and other U.S. government officials was performed. This included all Deputy Secretaries, Under Secretaries, Assistant Secretaries, Ambassadors-at-Large, Special Representatives and Envoys, members of the Secretary's Foreign Policy Advisory Board, and other senior officials to the Secretary, including close aides and staff.

Next, to account for non-obvious or non-recognizable email addresses or misspellings or other idiosyncrasies, the emails were sorted and reviewed both by sender and recipient.

Lastly, a number of terms were specifically searched for, including: "Benghazi" and "Libya."

These additional three steps yielded just over another 2,900 emails, including emails from former Administration officials and long-time friends that may not be deemed by the State Department to be federal records. And hundreds of these emails actually had already been forwarded onto the state.gov system and captured in real-time.

With respect to materials that the Select Committee has requested, the State Department has stated that just under 300 emails related to Libya were provided by the State Department to the Select Committee in response to a November 2014 letter, which contained a broader request for materials than prior requests from the House Oversight and Government Reform Committee.

Given Clinton's practice of emailing State Department officials on their state.gov addresses, the State Department already had, and had already provided, the Select Committee with emails from Clinton in August 2014 – prior to requesting and receiving printed copies of her emails.

The review process described above confirmed Clinton's practice of emailing State Department officials on their .gov address, with the vast majority of the printed copies of work-related emails Clinton provided to the State Department simply duplicating what was already captured in the State Department's record-keeping system in real time.

Did Clinton use this account to communicate with foreign officials?

During her time at State, she communicated with foreign officials in person, through correspondence, and by telephone. The review of all of her emails revealed only one email with a foreign (UK) official.

Did she withhold any work emails? What about the 15 emails that Sid Blumenthal provided to the Select Committee that she did not provide to the State Department?

She provided the State Department with all work and potentially work-related emails that she had, including all of her correspondence with Sid Blumenthal. We understand that Mr. Blumenthal had some emails that Clinton did not have, and Clinton had some emails that Mr. Blumenthal did not have, but it is important to note that none of those emails provide any new insights on the attack on our facilities in Benghazi.

Do you think a third party should have been allowed to review what was turned over to the State Department, as well as the remainder that was not?

The Federal Records Act puts the obligation on the government official, not the agency or a third party, to determine what is and is not a federal record. The State Department Foreign Affairs Manual outlines guidance "designed to help employees determine which of their e-mail messages must be preserved as federal records and which may be deleted without further authorization because they are not Federal record materials." [5 FAM 443.1(c)].

Clinton responded to the State Department's request by providing approximately 55,000 pages of her work and potentially work-related emails. She has also taken the unprecedented step of asking that those emails be made public. In doing so, she has sought to support the State Department's efforts, fulfill her responsibility of record-keeping, and provide the chance for the public to assess the work she and officials at the State Department did during her tenure.

After her work-related emails were identified and preserved, Clinton chose not to keep her private, personal emails that were not federal records, including emails about her daughter's wedding plans, her mother's funeral service, family vacations, etc.

Government officials are granted the privacy of their personal, non-work related emails, including personal emails on .gov accounts. Clinton exercised her privilege to ensure the continued privacy of her personal, non-work related emails.

Can't she release the emails she provided to the State Department herself?

Because the printed copies of work-related emails she provided to the State Department include federal records of the Department, the Department needs to review these emails before they can be made public. She called for them to be made available as soon as possible, and is glad to see the Department has begun releasing them.

Some of the emails released show Clinton emailed aides at times on their personal, rather than .gov accounts. Was she trying to hide these communications?

As Clinton has said before, it was her practice to email U.S. government officials on their .gov accounts if it was work-related. This is evidenced in the emails released so far. In reviewing her emails in 2014, there was a fraction of emails with work-related information sent to U.S. government officials' personal accounts, and those were provided to the State Department. The overwhelming majority of her work-related emails were to .gov accounts.

Where was the server for her email located?

The server for her email was physically located on her property, which is protected by U.S. Secret Service.

What level of encryption was employed? Who was the service provider?

The security and integrity of her family's electronic communications was taken seriously from the onset when it was first set up for President Clinton's team. While the curiosity about the specifics of this set up is understandable, given what people with ill intentions can do with such information in this day and age, there are concerns about broadcasting specific technical details about past and current practices. Suffice it to say, robust protections were put in place and additional upgrades and techniques employed over time as they became available, including consulting and employing third party experts.

Was the server ever hacked?

No, there is no evidence there was ever a breach.

Was there ever an unauthorized intrusion into her email or did anyone else have access to it?

No.

What was done after her email was exposed in February 2013 after the hacker known as "Guccifer" hacked Sid Blumenthal's account?

While this was not a breach of Clinton's account, because her email address was exposed, steps were taken at that time to ensure the security and integrity of her electronic communications, including changing her email address.

Was the State Department able to respond to requests related to FOIA or Congressional requests before they received printed copies of her work-related emails?

Yes. As the Select Committee has said, the State Department provided the Committee with relevant emails it already had on the state.gov system before the State Department requested any printed copies from former Secretaries, and four months before the State Department received the printed copies.

For example, in the well-publicized hack of Sid Blumenthal's email account, a note he sent Clinton on September 12, 2012, was posted online. At first blush, one might not think this exchange would be captured on the state.gov system. But in fact, Clinton forwarded the email, that very same day, onto the state.gov system. And the email was produced by the State Department to the Select Committee, and acknowledged by the Select Committee, in August 2014.

This example illustrates: 1) when an email from a non-".gov" sender had some connection to work or might add to the understanding of State Department officials, it was Clinton's practice to forward it to officials at their "state.gov" address; and 2) the State Department was able to search and produce Clinton's emails when needed long before, and unrelated to, receiving the printed copies as they were already captured on state.gov accounts.

SHARE THIS!

TWEET THIS!

22

FD-340 (Rev. 4-11-03)

File Number

CYBER-1A

b6
b7C

Field Office Acquiring Evidence WFO

Serial # of Originating Document

CYBER-31

Date Received 05/26/2016

From MARCEL LEHEL LAZAR

(Name of Contributor/Interviewee)

(Address)

(City and State)

By SA

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

**Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure**

☐ **Yes**☒ No**Federal Taxpayer Information (FTI)**☐ Yes☒ No

1A22

Reference: NOTES FROM INTERVIEW (FD-302)

(Communication Enclosing Material)

Description: ☒ Original notes re interview of

MARCEL LEHEL LAZAR

HRC-9101

MARIELE LAZAR

4/19.

5/26/16

2003 - 5/14 - Monday - 6:00am Pm.

- [redacted] - Add Back [redacted] - SID BLUM. - 20 mins - ^{Sec} ^{b6} ^{b7C}
- 30,000 - 8:15 - 6-7 hours. East - Clarke Logan
- Download Attack maps - Mexico
- Hacking / Scumskat - Only IP - 127.0.0.1 (Internal AOL)
- Checked - Bluetooth - IP Scumskat - Angry IT - most common
- Didn't see it always - Reluctant hacker. - Prodigy.
- Microsoft - Broken - MAC Address - Connected Scumskat
- Option in software - Connects to Proxy -
- 6-7 hours - 2hr break -
- Prodigy / Pro ^{b6} ^{b7C}
- Only screen shot - SID almost no lower action - New Testament ^{5th} ^{8th} ^{9th} ^{10th} ^{11th} ^{12th} ^{13th} ^{14th} ^{15th} ^{16th} ^{17th} ^{18th} ^{19th} ^{20th} ^{21st} ^{22nd} ^{23rd} ^{24th} ^{25th} ^{26th} ^{27th} ^{28th} ^{29th} ^{30th} ^{31st} ^{32nd} ^{33rd} ^{34th} ^{35th} ^{36th} ^{37th} ^{38th} ^{39th} ^{40th} ^{41st} ^{42nd} ^{43rd} ^{44th} ^{45th} ^{46th} ^{47th} ^{48th} ^{49th} ^{50th} ^{51st} ^{52nd} ^{53rd} ^{54th} ^{55th} ^{56th} ^{57th} ^{58th} ^{59th} ^{60th} ^{61st} ^{62nd} ^{63rd} ^{64th} ^{65th} ^{66th} ^{67th} ^{68th} ^{69th} ^{70th} ^{71st} ^{72nd} ^{73rd} ^{74th} ^{75th} ^{76th} ^{77th} ^{78th} ^{79th} ^{80th} ^{81st} ^{82nd} ^{83rd} ^{84th} ^{85th} ^{86th} ^{87th} ^{88th} ^{89th} ^{90th} ^{91st} ^{92nd} ^{93rd} ^{94th} ^{95th} ^{96th} ^{97th} ^{98th} ^{99th} ^{100th} ^{101st} ^{102nd} ^{103rd} ^{104th} ^{105th} ^{106th} ^{107th} ^{108th} ^{109th} ^{110th} ^{111th} ^{112th} ^{113th} ^{114th} ^{115th} ^{116th} ^{117th} ^{118th} ^{119th} ^{120th} ^{121st} ^{122nd} ^{123rd} ^{124th} ^{125th} ^{126th} ^{127th} ^{128th} ^{129th} ^{130th} ^{131st} ^{132nd} ^{133rd} ^{134th} ^{135th} ^{136th} ^{137th} ^{138th} ^{139th} ^{140th} ^{141st} ^{142nd} ^{143rd} ^{144th} ^{145th} ^{146th} ^{147th} ^{148th} ^{149th} ^{150th} ^{151st} ^{152nd} ^{153rd} ^{154th} ^{155th} ^{156th} ^{157th} ^{158th} ^{159th} ^{160th} ^{161st} ^{162nd} ^{163rd} ^{164th} ^{165th} ^{166th} ^{167th} ^{168th} ^{169th} ^{170th} ^{171st} ^{172nd} ^{173rd} ^{174th} ^{175th} ^{176th} ^{177th} ^{178th} ^{179th} ^{180th} ^{181st} ^{182nd} ^{183rd} ^{184th} ^{185th} ^{186th} ^{187th} ^{188th} ^{189th} ^{190th} ^{191st} ^{192nd} ^{193rd} ^{194th} ^{195th} ^{196th} ^{197th} ^{198th} ^{199th} ^{200th} ^{201st} ^{202nd} ^{203rd} ^{204th} ^{205th} ^{206th} ^{207th} ^{208th} ^{209th} ^{210th} ^{211st} ^{212nd} ^{213th} ^{214th} ^{215th} ^{216th} ^{217th} ^{218th} ^{219th} ^{220th} ^{221st} ^{222nd} ^{223rd} ^{224th} ^{225th} ^{226th} ^{227th} ^{228th} ^{229th} ^{230th} ^{231st} ^{232nd} ^{233rd} ^{234th} ^{235th} ^{236th} ^{237th} ^{238th} ^{239th} ^{240th} ^{241st} ^{242nd} ^{243rd} ^{244th} ^{245th} ^{246th} ^{247th} ^{248th} ^{249th} ^{250th} ^{251st} ^{252nd} ^{253rd} ^{254th} ^{255th} ^{256th} ^{257th} ^{258th} ^{259th} ^{260th} ^{261st} ^{262nd} ^{263rd} ^{264th} ^{265th} ^{266th} ^{267th} ^{268th} ^{269th} ^{270th} ^{271st} ^{272nd} ^{273rd} ^{274th} ^{275th} ^{276th} ^{277th} ^{278th} ^{279th} ^{280th} ^{281st} ^{282nd} ^{283rd} ^{284th} ^{285th} ^{286th} ^{287th} ^{288th} ^{289th} ^{290th} ^{291st} ^{292nd} ^{293rd} ^{294th} ^{295th} ^{296th} ^{297th} ^{298th} ^{299th} ^{300th} ^{301st} ^{302nd} ^{303rd} ^{304th} ^{305th} ^{306th} ^{307th} ^{308th} ^{309th} ^{310th} ^{311st} ^{312nd} ^{313th} ^{314th} ^{315th} ^{316th} ^{317th} ^{318th} ^{319th} ^{320th} ^{321st} ^{322nd} ^{323rd} ^{324th} ^{325th} ^{326th} ^{327th} ^{328th} ^{329th} ^{330th} ^{331st} ^{332nd} ^{333rd} ^{334th} ^{335th} ^{336th} ^{337th} ^{338th} ^{339th} ^{340th} ^{341st} ^{342nd} ^{343rd} ^{344th} ^{345th} ^{346th} ^{347th} ^{348th} ^{349th} ^{350th} ^{351st} ^{352nd} ^{353rd} ^{354th} ^{355th} ^{356th} ^{357th} ^{358th} ^{359th} ^{360th} ^{361st} ^{362nd} ^{363rd} ^{364th} ^{365th} ^{366th} ^{367th} ^{368th} ^{369th} ^{370th} ^{371st} ^{372nd} ^{373rd} ^{374th} ^{375th} ^{376th} ^{377th} ^{378th} ^{379th} ^{380th} ^{381st} ^{382nd} ^{383rd} ^{384th} ^{385th} ^{386th} ^{387th} ^{388th} ^{389th} ^{390th} ^{391st} ^{392nd} ^{393rd} ^{394th} ^{395th} ^{396th} ^{397th} ^{398th} ^{399th} ^{400th} ^{401st} ^{402nd} ^{403rd} ^{404th} ^{405th} ^{406th} ^{407th} ^{408th} ^{409th} ^{410th} ^{411st} ^{412nd} ^{413th} ^{414th} ^{415th} ^{416th} ^{417th} ^{418th} ^{419th} ^{420th} ^{421st} ^{422nd} ^{423rd} ^{424th} ^{425th} ^{426th} ^{427th} ^{428th} ^{429th} ^{430th} ^{431st} ^{432nd} ^{433rd} ^{434th} ^{435th} ^{436th} ^{437th} ^{438th} ^{439th} ^{440th} ^{441st} ^{442nd} ^{443rd} ^{444th} ^{445th} ^{446th} ^{447th} ^{448th} ^{449th} ^{450th} ^{451st} ^{452nd} ^{453rd} ^{454th} ^{455th} ^{456th} ^{457th} ^{458th} ^{459th} ^{460th} ^{461st} ^{462nd} ^{463rd} ^{464th} ^{465th} ^{466th} ^{467th} ^{468th} ^{469th} ^{470th} ^{471st} ^{472nd} ^{473rd} ^{474th} ^{475th} ^{476th} ^{477th} ^{478th} ^{479th} ^{480th} ^{481st} ^{482nd} ^{483rd} ^{484th} ^{485th} ^{486th} ^{487th} ^{488th} ^{489th} ^{490th} ^{491st} ^{492nd} ^{493rd} ^{494th} ^{495th} ^{496th} ^{497th} ^{498th} ^{499th} ^{500th} ^{501st} ^{502nd} ^{503rd} ^{504th} ^{505th} ^{506th} ^{507th} ^{508th} ^{509th} ^{510th} ^{511st} ^{512nd} ^{513th} ^{514th} ^{515th} ^{516th} ^{517th} ^{518th} ^{519th} ^{520th} ^{521st} ^{522nd} ^{523rd} ^{524th} ^{525th} ^{526th} ^{527th} ^{528th} ^{529th} ^{530th} ^{531st} ^{532nd} ^{533rd} ^{534th} ^{535th} ^{536th} ^{537th} ^{538th} ^{539th} ^{540th} ^{541st} ^{542nd} ^{543rd} ^{544th} ^{545th} ^{546th} ^{547th} ^{548th} ^{549th} ^{550th} ^{551st} ^{552nd} ^{553rd} ^{554th} ^{555th} ^{556th} ^{557th} ^{558th} ^{559th} ^{560th} ^{561st} ^{562nd} ^{563rd} ^{564th} ^{565th} ^{566th} ^{567th} ^{568th} ^{569th} ^{570th} ^{571st} ^{572nd} ^{573rd} ^{574th} ^{575th} ^{576th} ^{577th} ^{578th} ^{579th} ^{580th} ^{581st} ^{582nd} ^{583rd} ^{584th} ^{585th} ^{586th} ^{587th} ^{588th} ^{589th} ^{590th} ^{591st} ^{592nd} ^{593rd} ^{594th} ^{595th} ^{596th} ^{597th} ^{598th} ^{599th} ^{600th} ^{601st} ^{602nd} ^{603rd} ^{604th} ^{605th} ^{606th} ^{607th} ^{608th} ^{609th} ^{610th} ^{611st} ^{612nd} ^{613th} ^{614th} ^{615th} ^{616th} ^{617th} ^{618th} ^{619th} ^{620th} ^{621st} ^{622nd} ^{623rd} ^{624th} ^{625th} ^{626th} ^{627th} ^{628th} ^{629th} ^{630th} ^{631st} ^{632nd} ^{633rd} ^{634th} ^{635th} ^{636th} ^{637th} ^{638th} ^{639th} ^{640th} ^{641st} ^{642nd} ^{643rd} ^{644th} ^{645th} ^{646th} ^{647th} ^{648th} ^{649th} ^{650th} ^{651st} ^{652nd} ^{653rd} ^{654th} ^{655th} ^{656th} ^{657th} ^{658th} ^{659th} ^{660th} ^{661st} ^{662nd} ^{663rd} ^{664th} ^{665th} ^{666th} ^{667th} ^{668th} ^{669th} ^{670th} ^{671st} ^{672nd} ^{673rd} ^{674th} ^{675th} ^{676th} ^{677th} ^{678th} ^{679th} ^{680th} ^{681st} ^{682nd} ^{683rd} ^{684th} ^{685th} ^{686th} ^{687th} ^{688th} ^{689th} ^{690th} ^{691st} ^{692nd} ^{693rd} ^{694th} ^{695th} ^{696th} ^{697th} ^{698th} ^{699th} ^{700th} ^{701st} ^{702nd} ^{703rd} ^{704th} ^{705th} ^{706th} ^{707th} ^{708th} ^{709th} ^{710th} ^{711st} ^{712nd} ^{713th} ^{714th} ^{715th} ^{716th} ^{717th} ^{718th} ^{719th} ^{720th} ^{721st} ^{722nd} ^{723rd} ^{724th} ^{725th} ^{726th} ^{727th} ^{728th} ^{729th} ^{730th} ^{731st} ^{732nd} ^{733rd} ^{734th} ^{735th} ^{736th} ^{737th} ^{738th} ^{739th} ^{740th} ^{741st} ^{742nd} ^{743rd} ^{744th} ^{745th} ^{746th} ^{747th} ^{748th} ^{749th} ^{750th} ^{751st} ^{752nd} ^{753rd} ^{754th} ^{755th} ^{756th} ^{757th} ^{758th} ^{759th} ^{760th} ^{761st} ^{762nd} ^{763rd} ^{764th} ^{765th} ^{766th} ^{767th} ^{768th} ^{769th} ^{770th} ^{771st} ^{772nd} ^{773rd} ^{774th} ^{775th} ^{776th} ^{777th} ^{778th} ^{779th} ^{780th} ^{781st} ^{782nd} ^{783rd} ^{784th} ^{785th} ^{786th} ^{787th} ^{788th} ^{789th} ^{790th} ^{791st} ^{792nd} ^{793rd} ^{794th} ^{795th} ^{796th} ^{797th} ^{798th} ^{799th} ^{800th} ^{801st} ^{802nd} ^{803rd} ^{804th} ^{805th} ^{806th} ^{807th} ^{808th} ^{809th} ^{810th} ^{811st} ^{812nd} ^{813th} ^{814th} ^{815th} ^{816th} ^{817th} ^{818th} ^{819th} ^{820th} ^{821st} ^{822nd} ^{823rd} ^{824th} ^{825th} ^{826th} ^{827th} ^{828th} ^{829th} ^{830th} ^{831st} ^{832nd} ^{833rd} ^{834th} ^{835th} ^{836th} ^{837th} ^{838th} ^{839th} ^{840th} ^{841st} ^{842nd} ^{843rd} ^{844th} ^{845th} ^{846th} ^{847th} ^{848th} ^{849th} ^{850th} ^{851st} ^{852nd} ^{853rd} ^{854th} ^{855th} ^{856th} ^{857th} ^{858th} ^{859th} ^{860th} ^{861st} ^{862nd} ^{863rd} ^{864th} ^{865th} ^{866th} ^{867th} ^{868th} ^{869th} ^{870th} ^{871st} ^{872nd} ^{873rd} ^{874th} ^{875th} ^{876th} ^{877th} ^{878th} ^{879th} ^{880th} ^{881st} ^{882nd} ^{883rd} ^{884th} ^{885th} ^{886th} ^{887th} ^{888th} ^{889th} ^{890th} ^{891st} ^{892nd} ^{893rd} ^{894th} ^{895th} ^{896th} ^{897th} ^{898th} ^{899th} ^{900th} ^{901st} ^{902nd} ^{903rd} ^{904th} ^{905th} ^{906th} ^{907th} ^{908th} ^{909th} ^{910th} ^{911st} ^{912nd} ^{913th} ^{914th} ^{915th} ^{916th} ^{917th} ^{918th} ^{919th} ^{920th} ^{921st} ^{922nd} ^{923rd} ^{924th} ^{925th} ^{926th} ^{927th} ^{928th} ^{929th} ^{930th} ^{931st} ^{932nd} ^{933rd} ^{934th} ^{935th} ^{936th} ^{937th} ^{938th} ^{939th} ^{940th} ^{941st} ^{942nd} ^{943rd} ^{944th} ^{945th} ^{946th} ^{947th} ^{948th} ^{949th} ^{950th} ^{951st} ^{952nd} ^{953rd} ^{954th} ^{955th} ^{956th} ^{957th} ^{958th} ^{959th} ^{960th} ^{961st} ^{962nd} ^{963rd} ^{964th} ^{965th} ^{966th} ^{967th} ^{968th} ^{969th} ^{970th} ^{971st} ^{972nd} ^{973rd} ^{974th} ^{975th} ^{976th} ^{977th} ^{978th} ^{979th} ^{980th} ^{981st} ^{982nd} ^{983rd} ^{984th} ^{985th} ^{986th} ^{987th} ^{988th} ^{989th} ^{990th} ^{991st} ^{992nd} ^{993rd} ^{994th} ^{995th} ^{996th} ^{997th} ^{998th} ^{999th} ^{1000th}

- 100. MASTER

- MAKING VIRUS - SPARK PIRATE - RAT

- WOUND HIS OWN

- MIX TABLE - SPLIT INTO SMALL PIECES / CHANGING

- CLINSON

- RAT - TOOL MARK

- EVILGARD 7 - RAT TOOL USED

- ROBERTSON FAMILY - A LOT

- BACK FROM

- VIRUS HAS KEYLOGGERS

- RICHIE SAYS OF KEYLOGGERS 10/9

- 100 PEOPLE WERE (IS OPENING)

- ~~THE~~ DIDN'T HAVE TRAVE ACCOUNTS

- DIDN'T GET TO CLINSON DOMAIN

- 2009-2010 - Facebook Account HIPRO - Desktop screenshots

- MATE

- WINDOWS - COMMAND PROMPT

- FROM BROWSER - MONITOR ALL ACTIVITIES FROM BROWSER

- DIFFERENT COMPUTERS - USED SINCE 15 YEARS OLD

CAW/ABOVE - ANDREW OR

DATES

ANGRY IP IN 6/2013?

COINBON ACTIVITIES IN 03/2013 / 06/2013? - One Day after

CARIN + ASKE - Password cracking?

- 3/14/2013 - Same day (FAT2)

- 3/15/2013 -

[] - LINE ACCOUNTS - Password []

- 06/2013 - Did not have IP b6
b7C

- Secondary Account - STILL UNABLE

- Account Phone call to AOL

- [] - Don't remember.

- Never ran Angry IP - Never had IP Address

- Never ran Angry IP Against.

- CARIN + ASKE - GUI & Green / Red Buttons

- Can't describe - 2010/2011

- Script KIDNAPES

- DOWNW - Panniden

- XALWIN - Log into servers

- Don't remember

- Browser - Didn't know -

- IP Scanner

- Clean up - Not delete - No logs.

- AMATUER

#23

FD-340 (Rev. 4-11-03)

File Number

[Redacted]

- CYBER-1A -

b3
b7E

Field Office Acquiring Evidence WFO

Serial # of Originating Document

[Redacted]

- CYBER-32

Date Received 06/02/2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

SA

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A23

Reference: FD-1057 dated 06/02/2016

(Communication Enclosing Material)

Description: ☐ Original notes re interview of

TWO (2) FOX NEWS articles, dated 03/04/2016

and 03/07/2016.

HRC-9105

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-20-2017 BY J76J18T80 NSICG



Print Close

Romanian hacker Guccifer: I breached Clinton server, 'it was easy'

By Catherine Herridge, Pamela K. Browne

Published May 04, 2016

FoxNews.com

EXCLUSIVE: The infamous Romanian hacker known as "Guccifer," speaking exclusively with Fox News, claimed he easily — and repeatedly — breached former Secretary of State Hillary Clinton's personal email server in early 2013.

"For me, it was easy — easy for me, for everybody," Marcel Lehel Lazar, who goes by the moniker "Guccifer," told Fox News from a Virginia jail where he is being held.

Guccifer's potential role in the Clinton email investigation was first reported by Fox News last month. The hacker subsequently claimed he was able to access the server — and provided extensive details about how he did it and what he found — over the course of a half-hour jailhouse interview and a series of recorded phone calls with Fox News.

Fox News could not independently confirm Lazar's claims.

In response to Lazar's claims, the Clinton campaign issued a statement Wednesday night saying, "There is absolutely no basis to believe the claims made by this criminal from his prison cell. In addition to the fact he offers no proof to support his claims, his descriptions of Secretary Clinton's server are inaccurate. It is unfathomable that he would have gained access to her emails and not leaked them the way he did to his other victims."

The former secretary of state's server held nearly 2,200 emails containing information now deemed classified, and another 22 at the "Top Secret" level.

2016 Election Headquarters

The latest headlines on the 2016 elections from the biggest name in politics. [See Latest Coverage →](#)

The 44-year-old Lazar said he first compromised Clinton confidant Sidney Blumenthal's AOL account, in March 2013, and used that as a stepping stone to the Clinton server. He said he accessed Clinton's server "like twice," though he described the contents as "not interest[ing]" to him at the time.

"I was not paying attention. For me, it was not like the Hillary Clinton server, it was like an email server she and others were using with political voting stuff," Guccifer said.

The hacker spoke freely with Fox News from the detention center in Alexandria, Va., where he's been held since his extradition to the U.S. on federal charges relating to other alleged cyber-crimes. Wearing a green jumpsuit, Lazar was relaxed and polite in the monitored secure visitor center, separated by thick security glass.

In describing the process, Lazar said he did extensive research on the web and then guessed Blumenthal's security question. Once inside Blumenthal's account, Lazar said he saw dozens of messages from the Clinton email address.

Asked if he was curious about the address, Lazar merely smiled. Asked if he used the same security question approach to access the Clinton emails, he said no — then described how he allegedly got inside.

"For example, when Sidney Blumenthal got an email, I checked the email pattern from Hillary Clinton, from Colin Powell from anyone else to find out the originating IP. . . When they send a letter, the email header is the originating IP usually," Lazar explained.

He said, "then I scanned with an IP scanner."

Lazar emphasized that he used readily available web programs to see if the server was "alive" and which ports were open. Lazar identified programs like netscan, Netmap, Wireshark and Angry IP, though it was not possible to confirm independently which, if any, he used.

In the process of mining data from the Blumenthal account, Lazar said he came across evidence that others were on the Clinton server.

"As far as I remember, yes, there were ... up to 10, like, IPs from other parts of the world," he said

With no formal computer training, he did most of his hacking from a small Romanian village.

Lazar said he chose to use "proxy servers in Russia," describing them as the best, providing anonymity

Cyber experts who spoke with Fox News said the process Lazar described is plausible. The federal indictment Lazar faces in the U.S. for cyber-crimes specifically alleges he used "a proxy server located in Russia" for the Blumenthal compromise.

Each Internet Protocol (IP) address has a unique numeric code, like a phone number or home address. The Democratic presidential front-runner's home-brew private server was reportedly installed in her home in Chappaqua, N.Y., and used for all U.S. government business during her term as secretary of state.

Former State Department IT staffer Bryan Pagliano, who installed and maintained the server, has been granted immunity by the Department of Justice and is cooperating with the FBI in its ongoing criminal investigation into Clinton's use of the private server. An intelligence source told Fox News last month that Lazar also could help the FBI make the case that Clinton's email server may have been compromised by a third party.

Asked what he would say to those skeptical of his claims, Lazar cited "the evidence you can find in the Guccifer archives as far as I can remember."

Writing under his alias Guccifer, Lazar released to media outlets in March 2013 multiple exchanges between Blumenthal and Clinton. They were first reported by the Smoking Gun.

It was through the Blumenthal compromise that the Clintonemail.com accounts were first publicly revealed.

As recently as this week, Clinton said neither she nor her aides had been contacted by the FBI about the criminal investigation. Asked whether the server had been compromised by foreign hackers, she told MSNBC on Tuesday, "No, not at all."

Recently extradited, Lazar faces trial Sept. 12 in the Eastern District of Virginia. He has pleaded not guilty to a nine-count federal indictment for his alleged hacking crimes in the U.S. Victims are not named in the indictment but reportedly include Colin Powell, a member of the Bush family and others including Blumenthal.

Lazar spoke extensively about Blumenthal's account, noting his emails were "interesting" and had information about "the Middle East and what they were doing there."

After first writing to the accused hacker on April 19, Fox News accepted two collect calls from him, over a seven-day period, before meeting with him in person at the jail. During these early phone calls, Lazar was more guarded.

After the detention center meeting, Fox News conducted additional interviews by phone and, with Lazar's permission, recorded them for broadcast.

While Lazar's claims cannot be independently verified, three computer security specialists, including two former senior intelligence officials, said the process described is plausible and the Clinton server, now in FBI custody, may have an electronic record that would confirm or disprove Guccifer's claims.

"This sounds like the classic attack of the late 1990s. A smart individual who knows the tools and the technology and is looking for glaring weaknesses in Internet-connected devices," Bob Gourley, a former chief technology officer (CTO) for the Defense Intelligence Agency, said.

Gourley, who has worked in cybersecurity for more than two decades, said the programs cited to access the server can be dual purpose. "These programs are used by security professionals to make sure systems are configured appropriately. Hackers will look and see what the gaps are, and focus their energies on penetrating a system," he said.

Cybersecurity expert Morgan Wright observed, "The Blumenthal account gave [Lazar] a road map to get to the Clinton server. You get a foothold in one system. You get intelligence from that system, and then you start to move."

In March, the New York Times reported the Clinton server security logs showed no evidence of a breach. On whether the Clinton security logs would show a compromise, Wright made the comparison to a bank heist. "Let's say only one camera was on in the bank. If you don't have them all on, or the right one in the right locations, you won't see what you are looking for."

Gourley said the logs may not tell the whole story and the hard drives, three years after the fact, may not have a lot of related data left. He also warned: "Unfortunately, in this community, a lot of people make up stories and it's hard to tell what's really true until you get into the forensics information and get hard facts."

For Lazar, a plea agreement where he cooperates in exchange for a reduced sentence would be advantageous. He told Fox News he has nothing to hide and wants to cooperate with the U.S. government, adding that he has hidden two gigabytes of data that is "too hot" and "it is a matter of national security."

In early April, at the time of Lazar's extradition from a Romanian prison where he already was serving a seven-year sentence for cyber-crimes, a former senior FBI official said the timing was striking.

"Because of the proximity to Sidney Blumenthal and the activity involving Hillary's emails, [the timing] seems to be something beyond curious," said Ron Hosko, former assistant director of the FBI's Criminal Investigative Division from 2012-2014.

The FBI offered no statement to Fox News.

Catherine Herridge is an award-winning Chief Intelligence correspondent for FOX News Channel (FNC) based in Washington, D.C. She covers intelligence, the Justice Department and the Department of Homeland Security. Herridge joined FNC in 1996 as a London-based correspondent.

Pamela K. Browne is Senior Executive Producer at the FOX News Channel (FNC) and is Director of Long-Form Series and Specials. Her journalism has been recognized with several awards. Browne first joined FOX in 1997 to launch the news magazine "Fox Files" and later, "War Stories."

 Print  Close

URL

<http://www.foxnews.com/politics/2016/05/04/romanian-hacker-guccifer-breached-clinton-server-it-was-easy.html>

[Home](#) | [Video](#) | [Politics](#) | [U.S.](#) | [Opinion](#) | [Entertainment](#) | [Tech](#) | [Science](#) | [Health](#) | [Travel](#) | [Lifestyle](#) | [World](#) | [Sports](#) | [Weather](#)

[Privacy](#) | [Terms](#)

This material may not be published, broadcast, rewritten, or redistributed. © FOX News Network, LLC. All rights reserved. All market data delayed 20 minutes.

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 01-20-2017 BY J76J18T80 NSICG

Print Close



Romanian hacker who claims he breached Clinton server says he spoke with FBI at length

By Catherine Hemidge, Pamela K. Browne

Published May 07, 2016

FoxNews.com

EXCLUSIVE: The Romanian hacker who says he easily breached Hillary Clinton's personal email server also claimed, in a series of interviews with Fox News, that he spoke with the FBI at length on the plane when extradited from Romania to Virginia last month.

"They came after me, a guy from the FBI, from the State Department," 44-year-old Marcel Lehel Lazar, who goes by the moniker "Guccifer," told Fox News during a jailhouse phone interview. He said the conversation was "80 minutes recorded," and he took his own notes.

A government source confirmed that the hacker had a lot to say on the plane but provided no other details. Lazar was flown to the U.S. to face separate cyber-crime charges.

In addition to the apparent conversation with the FBI on the plane, Fox News has learned a meeting was expected as early as this week at the Alexandria, Va., detention center where he's being held involving Guccifer, the FBI, the U.S. attorney and the defendant's court-appointed lawyer.

These officials have not commented on his claims or detention.

An intelligence source close to the investigation, speaking with Fox News last month, questioned the timing of Lazar's extradition to the U.S., coming amid the Clinton email probe. As for what was discussed on that plane, Lazar said he told a State Department representative on the plane about "hot" data, some of which was hidden in Google drives, and other data that was too sensitive and deleted. The hacker, who offered no proof for his claims, said cryptically that he could not say more.

"I can't tell [you] now. I can't tell because I want to talk to the FBI. It is a matter of national security. Yeah," he said. Pressed by Fox News, Lazar seemed to indicate the data was not connected to the ongoing FBI criminal probe of Clinton's server.

Fox News recently met with Lazar in the secure visitor center in Alexandria, then followed up with a series of phone calls which he gave permission to be recorded. Separated by reinforced glass, Lazar was polite and methodical as he explained how he allegedly accessed the Clinton server in early 2013, by using her longtime confidant Sidney Blumenthal's AOL account as a stepping stone.

Fox News was first to report the hacker's claims of accessing the Clinton server, which he said "was easy."

Lazar said he got into the Blumenthal account by correctly guessing his security question, after doing extensive research on the web. He said his hacking always followed a "four step process": identify the target, do extensive web research on the target, access the target's account to harvest data, and send it out to the media.

Lazar said he was puzzled by the American media. He said he sent the Blumenthal emails, which is how the Clintonemail.com account first came to light, to many large news organizations in 2013, and it was The Smoking Gun that picked it up. Lazar said he started his "Guccifer archive," releasing materials in October and November 2012, and it ended "like August 2013."

Three cybersecurity experts said they found Lazar's explanation for accessing the Clinton server plausible but had questions.

Cybersecurity expert Morgan Wright explained how the FBI could marry up available evidence, including forensics or the configuration of the server and its folders, to assess his claims. "So we're going to map these things together, and if those things match up together, they're going to say 'yes, this was compromised,' then it means it was open to other people to compromise as well," he said.

Since Fox News reported on Guccifer's claims Wednesday, anonymous sources have reported that a review of the Clinton hard drives does not appear to indicate a breach. However, Wright and other experts warned that Clinton IT specialist Bryan Pagliano was the server's administrator and not principally a cybersecurity specialist — and may not have installed an adequate detection system for a Cabinet secretary's email.

"If you have a bank and you have one video camera when you need 20, then you missed it," Wright said. "If they weren't capturing

HRC-9109

all the activity their security logs may say they didn't see anything."

Asked about Lazar's claims at Thursday's press briefing, State Department spokesman Mark Toner also said he's not aware of such an incident.

"We don't have any reason to believe that it might be true," he said.

At the same time, Toner repeatedly stressed he did not want to comment on the security of the server, citing ongoing investigations. Asked if he's in a position to even know whether Lazar's claims are true, Toner again said he did not want to comment. The Clinton campaign has rejected Lazar's claims, calling them "baseless" and emphasizing he is a convicted hacker.

Other cyber specialists like Bob Gourley with Cognito warned there will "always be uncertainty and ambiguity" with hackers like Guccifer. But he said: "One thing I would say with certainty however -- if this computer were in a well-managed facility, where everything was being monitored and watched, we would have more information and ground truth."

Catherine Herridge is an award-winning Chief Intelligence correspondent for FOX News Channel (FNC) based in Washington, D.C. She covers intelligence, the Justice Department and the Department of Homeland Security. Herridge joined FNC in 1996 as a London-based correspondent.

Pamela K. Browne is Senior Executive Producer at the FOX News Channel (FNC) and is Director of Long-Form Series and Specials. Her journalism has been recognized with several awards. Browne first joined FOX in 1997 to launch the news magazine "Fox Files" and later, "War Stories."

 Print  Close

URL

<http://www.foxnews.com/politics/2016/05/07/romanian-hacker-who-claims-breached-clinton-server-says-spoke-with-fbi-at-length.html>

[Home](#) | [Video](#) | [Politics](#) | [U.S.](#) | [Opinion](#) | [Entertainment](#) | [Tech](#) | [Science](#) | [Health](#) | [Travel](#) | [Lifestyle](#) | [World](#) | [Sports](#) | [Weather](#)

[Privacy](#) | [Terms](#)

This material may not be published, broadcast, rewritten, or redistributed. © FOX News Network, LLC. All rights reserved. All market data delayed 20 minutes.

#24

FD-340 (Rev 4-11-03)

File Number

[REDACTED]

-CYBER-1A-

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[REDACTED]

-CYBER-33

Date Received

17 JUNE 2016

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

1A

[REDACTED]

(CYD)

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A24

Reference:

FD-1057 DATED 17 JUNE 2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

PRINTOUTS OF THREE .TXT FILES FOUND

ON PAGLIANO'S DESKTOP.

HRC-9111

b3
b7E

b6
b7C

#25

FD-340 (Rev 4-11-03)

File Number

[Redacted]

- CYBER

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

34

Date Received

13 MC
6/21/2016

From

ITS/FE

[Redacted]

(Name of Contributor/Interviewee)

b6
b7C

(Address)

(City and State)

By

ITS/FE

[Redacted]

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A25

(U)

~~(S/HF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Reference:

(Communication Enclosing Material)

Description:

☒ Original notes re interview of MC

DVD containing

[Redacted]

for

the time period of January 7 - 10, 2011

b7E

HRC-9120

- CYBER-1A -

WFO

-CYBER- 35

06/23/2016

(Address)

1A

☒ No☒ No☐ Yes☒ No☐ Yes☒ No

1A26

(Communication Enclosing Material)

☒ Original notes re interview of

HRC-9121

#27

FD-340 (Rev 4-11-03)

File Number

[REDACTED] CYBER-1A-

b3
b7E

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[REDACTED] CYBER-37

Date Received

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

IA

[REDACTED]

(CYD)

b6
b7C

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)

Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A27

Reference:

FD-1057 DATED 07/06/2016

(Communication Enclosing Material)

Description:

☐

Original notes re interview of

disc containing excel spreadsheet of IIS logs

related to

[REDACTED]

e-mail account

for January 5, 2013.

b6
b7C

HRC-91391

FD-340 (Rev 4-11-03)

File Number

[Redacted]

CYBER-1A-

Field Office Acquiring Evidence

WFO

Serial # of Originating Document

[Redacted]

CYBER-38

Date Received

07/15/16

From

(Name of Contributor/Interviewee)

(Address)

(City and State)

By

1A

[Redacted]

(CYD)

To Be Returned ☐ Yes

☒ No

Receipt Given ☐ Yes

☒ No

Grand Jury Material - Disseminate Only Pursuant to Rule 6 (e)
Federal Rules of Criminal Procedure

☐ Yes

☒ No

Federal Taxpayer Information (FTI)

☐ Yes

☒ No

1A28

Reference:

FD-1057 DATED 07/15/16

(Communication Enclosing Material)

Description:

☐ Original notes re interview of

- DISC WITH BP ITS LOGS FOR "H" ACCOUNTS,
PROVIDED BY DTD ON 06/17/16.

- DISC WITH BP ITS LOGS FOR "H" ACCOUNTS INFUSED
WITH IP ADDRESS RESOLUTIONS. DISC DATED 07/15/16.

HRC-9140

b3
b7E

b6
b7C

FD-1057 (Rev 5-8-10)

~~SECRET//NOFORN~~ (U)



FEDERAL BUREAU OF INVESTIGATION
Electronic Communication

Title: (U) Subfile Opening Document

Date: 10/08/2015

CC: [REDACTED]

b6
b7C

From: WASHINGTON FIELD

WF-CI13

Contact: [REDACTED]

b6
b7C

Approved By: [REDACTED]

Drafted By: [REDACTED]

Case ID #: [REDACTED] - FILTER (S//NF) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3
b7E

Synopsis: (U) To open a FILTER Subfile for material related to Filter process.

~~Reason: 1.4(c)
Derived From: Multiple
Sources
Declassify On: 20401231~~

Details:

To open a FILTER subfile for relevant information associated with the Filter process in captioned investigation.

◆◆

~~SECRET//NOFORN~~ (U)

HRC-9141

11/30/15
Serial 2

b6
b7c

HRC-9142

(Rev 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Title: (U//~~FOUO~~) To memorialize the Finalized Filter Team Memorandum from the Department of Justice

Date: 11/23/15

To: Washington Field

From: Washington Field

CI-12

Contact: SA [REDACTED]

b6
b7C

Approved By: SSA [REDACTED]

Drafted By: [REDACTED]

(U)

Case ID #: (~~S//NF~~) [REDACTED]-FILTER - 2

b3
b7E

(U) (~~S//NF~~) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To memorialize the Filter Team Memorandum dated October 28, 2015 provided by the U.S. Department of Justice National Security Division.

Enclosure(s): Enclosed are the following items:

1. (U//~~FOUO~~) Filter Team Memorandum dated 10/08/2015, and
2. (U//~~FOUO~~) Filter Team Memorandum with Attachment A dated 10/28/2015.

~~Classified By: F53M23K80
Derived From: FBI-NSIC dated 20130301
Declassify On: 20401231~~

Details: (U//~~FOUO~~) On October 8, 2015, the U.S. Department of Justice (DOJ) National Security Division, Counterintelligence and Export Control Section (CES) Trial Attorney [REDACTED] provided the FBI Filter Team with the enclosed copy of the Filter Team Instructions, dated the same. The Filter Team Instructions' Attachment A (Search Terms) had not yet been finalized at this time.

b6
b7C

~~SECRET//NOFORN~~

HRC-9143

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

b6
b7C

(U//~~FOUO~~) On October 8, 2015, [] reviewed the Filter Team Instructions with the Filter Team members. The Filter Team consisted of the following individuals from Washington Field Office (WFO): Special Agent (SA) [] SA [] SA [] Intelligence Analyst (IA) [] IA [] and IA [] the following attorney from FBI Headquarters (FBIHQ) National Security Law Branch (NSLB): Assistant General Counsel []; and Operational Technology Division (OTD) Information Technology Specialist / Forensic Examiner []. Also present for the duration of the briefing were WFO Assistant Special Agent in Charge (ASAC) Peter P. Strzok, Supervisory Special Agent (SSA) [] and FBIHQ Counterintelligence Division Assistant Section Chief (ASC) Jonathan Moffa.

b6
b7C

(U//~~FOUO~~) On October 28, 2015, [] provided the FBI Filter Team with the enclosed final version of the Filter Team Instructions, dated the same. The finalized version contains an additional attachment (Attachment A (Search Terms)).

♦♦

~~SECRET//NOFORN~~

4/11/16
Serial 3

b6
b7c

HRC-9145

(Rev 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Title: (U//~~FOUO~~) To memorialize the Addendum to the Filter Team Memorandum from the Department of Justice

Date: 04/01/16

To: Washington Field

From: Washington Field

CI-12

Contact: SA [REDACTED]

Approved By: SSA [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** (~~S//NF~~) [REDACTED] -FILTER - 3

(U) (~~IS//NF~~) MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

b3
b6
b7C
b7E

Synopsis: (U//~~FOUO~~) To memorialize the Addendum to the Filter Team Memorandum for Unallocated Space dated January 22, 2016 provided by the U.S. Department of Justice National Security Division.

Enclosure(s): Enclosed is the following item:

1. (U//~~FOUO~~) Filter Team Memorandum dated 01/22/2016

~~Classified By: F53M23K80~~

~~Derived From: FBI-NSIC dated 20130301~~

~~Declassify On: 20411231~~

Details: (U//~~FOUO~~) On January 22, 2016, the U.S. Department of Justice (DOJ) National Security Division, Counterintelligence and Export Control Section (CES) Trial Attorney [REDACTED] provided the FBI Filter Team with the enclosed copy of the Addendum to Filter Team Instructions Regarding Unallocated Space, dated the same.

b6
b7C

(U//~~FOUO~~) The Addendum changes were reviewed with the Filter Team on February 1, 2016 by FBI Headquarters (FBIHQ) National Security Law Branch (NSLB) Assistant General Counsel [REDACTED]. The

b6
b7C

~~SECRET//NOFORN~~

HRC-9146

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Addendum was also briefed to the Investigative Team on February 4, 2016 by [REDACTED].

b6
b7C

(U//~~FOUO~~) On March 24, 2016, [REDACTED] reviewed the collective Filter Team Instructions with new Filter Team members. The new Filter Team members consisted of the following individuals from Washington Field Office (WFO): Special Agent (SA) [REDACTED], SA [REDACTED] [REDACTED] and SA [REDACTED].

b6
b7C

♦♦

~~SECRET//NOFORN~~

4/14/16
serial 4

b6
b7c

HRC-9148

(Rev 05-01-2008)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

Title: (U//~~FOUO~~) To memorialize the review of case evidence by the Filter Team

Date: 04/11/16

To: Washington Field

From: Washington Field

CI-12

Contact: SA [REDACTED]

Approved By: SSA [REDACTED]

Drafted By: [REDACTED]

(U) **Case ID #:** ~~(S//NF)~~ [REDACTED] -FILTER -4

(U) ~~(S//NF)~~ MIDYEAR EXAM;
MISHANDLING OF CLASSIFIED;
UNKNOWN SUBJECT OR COUNTRY;
SENSITIVE INVESTIGATIVE MATTER (SIM)

Synopsis: (U//~~FOUO~~) To memorialize the review of case evidence by the Filter Team as of April 6, 2016.

~~Classified By: F53M23K80~~

~~Derived From: FBI NSIC dated 20130301~~

~~Declassify On: 20411231~~

Details: (U//~~FOUO~~) On or about September 30, 2015 through April 6, 2016, the designated Filter Team conducted a filter review of case evidence as directed by the Investigative Team. This evidence consisted entirely of digital media, which was processed by the Federal Bureau of Investigation (FBI) Operational Technology Division (OTD), and provided to the Filter Team [REDACTED]

[REDACTED]. The Filter Team conducted their review per the Memorandums provided by the Department of Justice (DOJ) and with guidance from the FBI National Security Law Branch (NSLB). The Filter Team passed the files deemed to be not privileged to the Investigative Team via OTD.

(U//~~FOUO~~) The evidence items that the Filter Team reviewed include the following:

~~SECRET//NOFORN~~

b3
b6
b7C
b7E

b7E

HRC-9149

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

- 1) 1B1 - (U) 1 Lexar micron 16 GB Black & Silver Thumbdrive - LJDTT166-000-1001 DA (Original), 1Lexar Micron 8 GB Green and White LJDTT8GB-000-117AU(Copy 1), 1 Kingston 8GB Silver DT SE9 (Copy 2)
- 2) 1B2 - (U) Lenovo Think Pad T420 PB-YC912 12/03
- 3) 1B3 - (U) Dell Poweredge 2900, Gray Color, S/N G842PC1
- (U) 4) 1B31 - (S) USB Thumbdrive
- (U) 5) 1B40 - (S) 1 Apple Mac Book Air Laptop S/N C0ZLF0ICFM74
- (U) 6) 1B43 - (S) Seagate Desktop External Hard Drive 1000 GB, S/N 2GHJ026M/Power Supply/USB Cable
- (U) 7) 1B44 - (S) Datto Server Supermicro 2V Server, Model 52000, S/N 002590AFDEBE, Invoice 482547
- (U) 8) 1B46 - (S) Q NAP Network Attached Storage (NAS) Device Model TS-1079 Pro, Serial #Q-11AI10175, 21.76 TB Total Capacity containing 1TB Data Loaded from PRN Servers & Equipment
- (U) 9) 1B47 - (S) Apple Mac Pro S/N W893361H6644, Power Cord
- (U) 10) 1B48 - (S) Server 882 Dattobackup.com barcode C8470FC11M70024, Pin #CSE847
- 11) 1B56 - (U) One (1) Western Digital My Passport Ultra External Hard Drive with Serial Number WXG1AA3M2130
- (U) 12) 1B64 - (S) 1 - 16GB SanDisk USB Drive
- 13) 1B71 - (U) One (1) iPad with Serial Number , IMEI 012224007843867

b6
b7C

(U//~~FOUO~~) Of the aforementioned items, items 1B3 and 1B43, contained over 200,000 unallocated files or file fragments available for Filter review. The review of the unallocated files was initially conducted in accordance with the Filter Team Instructions provided by DOJ on October 8, 2015, but the review quickly became unmanageable under those instructions. On or about December 8, 2015, the Investigative Team provided the Filter Team with a list of search terms to be used in to assist with narrowing the files that needed Filter review. The Investigative Team agreed that the Filter Team did not have to review any files that did not include a "hit" on a search term.

b7E

(U//~~FOUO~~) The Investigative Key Word Search Terms provided to the Filter Team on or about December 8, 2015 were as follows:

b7E

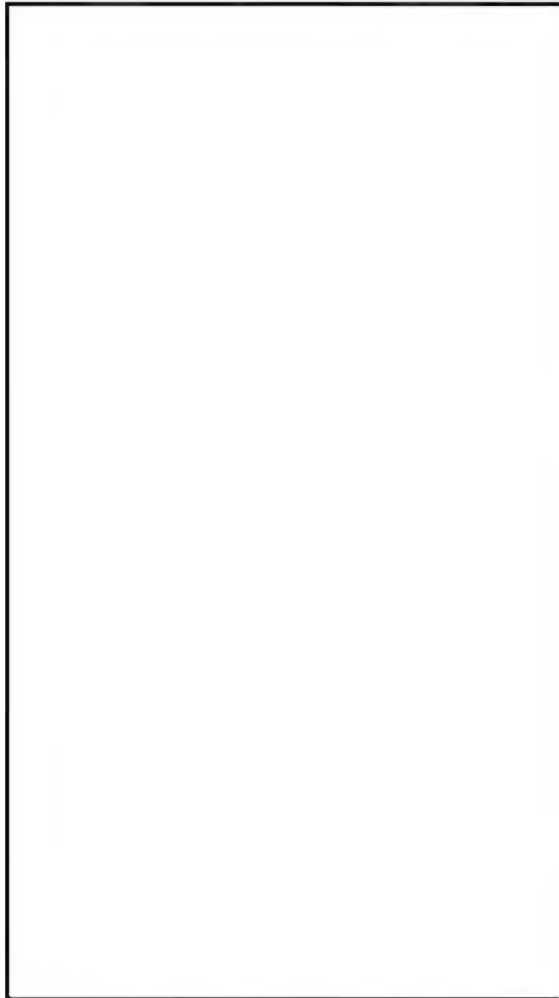


~~SECRET//NOFORN~~

~~SECRET//NOFORN~~ (U)

FEDERAL BUREAU OF INVESTIGATION

b7E



(U//~~FOUO~~) The Filter Team proceeded to use the Investigative Key Word Search Terms to conduct their review of the unallocated files, but the review still remained unmanageable. In addition, due to system limitations, the Filter Team encountered additional difficulty in opening and managing the larger-sized files (upwards of 500 MB).

b7E

(U//~~FOUO~~) DOJ provided an addendum set of instructions specific to the Filter review of unallocated files on or about January 22, 2016. Using the addendum instructions in conjunction with a revised set of Investigative Search Terms provided on or about February 1, 2016, and with OTD splitting the larger files into smaller files (200K or less), the Filter Team was able to complete their review.

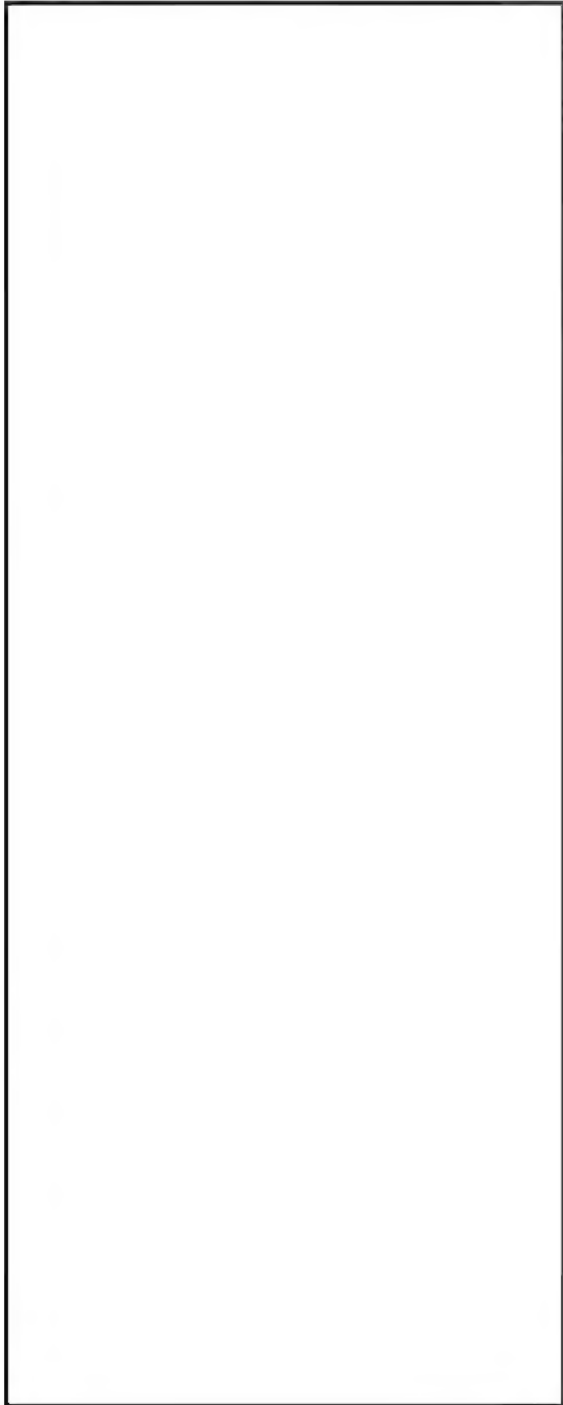
~~SECRET//NOFORN~~ (U)

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

(U//~~FOUO~~) The Investigative Key Word Search Terms provided to the Filter Team on or about February 1, 2016 were as follows:

b7E

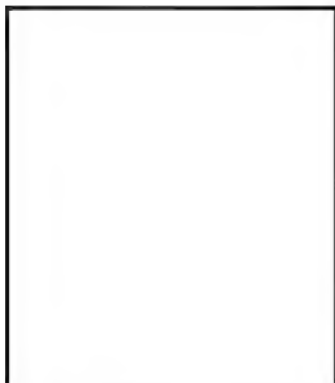


~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FEDERAL BUREAU OF INVESTIGATION

b7E



(U//~~FOUO~~) Based on the augmented instructions, the Filter Team completed their filter and quality control reviews of the unallocated files on or about April 7, 2016. From on or about September 30, 2015 through April 6, 2016, the Filter Team adjudicated over 45,000 files (files that had Filter Term hits) and passed over 750,000 files (that did not have Filter Term hits).

♦♦

~~SECRET//NOFORN~~

HRC-9153